공공정보의 이차 활용을 위한 법제도에 관한 연구

- 생체·의료정보의 이차 활용을 중심으로 -

연세대학교 대학원

의료법윤리학협동과정

보 건 학 전 공

박 미 정

공공정보의 이차 활용을 위한 법제도에 관한 연구

- 생체·의료정보의 이차 활용을 중심으로 -

지도 김 소 윤 교수

이 논문을 박사 학위논문으로 제출함

2014년 12월

연세대학교 대학원

의료법윤리학협동과정

보 건 학 전 공

박 미 정

박미정의 박사 학위논문을 인준함

심사위원 金昭允 (인)

심사위원 孫明世 (인)

심사위원 金正梧 (인)

심사위원 이일학 (인)

심사위원 김석일 (인)

연세대학교 대학원

2014년 12월

감사의 글

학위논문을 위한 연구는 저 혼자 고군분투하는 것이라기보다는 다른 사람의 의견을 얼마나 잘 청취 했는가를 보여주는 결과입니다. 다양한 전문분야의 교수님들, 대학캠퍼스와 이곳을 벗어나 함께 공부 했던 학형들, 보건의료현장에서 일하는 동료들 모두가 이 논문이 기반하고 있는 사상과 견해와 의미 있는 표현 하나하나를 형성하는데 기여했습니다. 무엇보다 학제간의 연구는 그 내용 뿐만 아니라 형식과 틀까지 소통하며 합의에 이르러야 하는 긴 과정을 필요로 했습니다.

그 누구보다 김소윤 교수님은 이 연구를 가능하게 했고, 없어서는 안 될 논문으로 만들 수 있도록 지도해 주셨습니다. 마무리 작업의 막바지에서 계속하여 수정을 거듭할 때 염려와 기대를 거두지 않고 함께 지켜 봐주셨던 김정오님의 지극한 애정에 감사드립니다. 그리고 날카로운 비판을 해주신 이일학 교수님, 보건의료정보학에서의 법학적 접근을 격려해 주신 김석일 교수님께 감사드립니다. 그리고 계속 연구할 수 있는 좋은 출발이 되게 해주신 손명세 건강보험심사평가원장님께 감사드립니다. 학위과정 내내 함께 했던 연세대학교 의료법윤리학연구원의 동료들에게도 감사드립니다.

흩어져 있는 데이터가 의미가 되도록 모으고, 비로소 누구에겐가 필요한 정보로 해석된다면, 질병이 예방되고 건강이 관리될 수 있겠다는 생각이 동기가 되어 보건의료분야에서 다시 학습하였습니다.

보건의료정보학도로서 정보의 활용측면만을 연구하다가, 현장에서 치열하게 경험할 수 있었습니다. 그러한 기회와 여건을 허락해 주신 많은 분들의 격려와 도움으로 이 연구가 가능하였습니다. 질병관리본부에서 일하는 동안 정보시스템을 만들고 조사하고 분석하여 가치 있는 정보를 제공하면서부터 공공정보의 활용에

대하여 고민하였습니다. 그리고 계속하여 지역사회에서부터 글로벌에 이르기까지 보건사업과 교육에 대해서 일할 수 있었습니다. 필요한 곳에서 계속 일할 수 있는 기회를 허락해 주신 서울대학교 의과대학 이종구 교수님께 감사드립니다. 함께 연구하였던 질병관리본부와 국립보건원 동료들께도 감사드립니다.

공공정보를 잘 활용하기 위해서는 프라이버시 보호를 고려하지 않으면 안 된다는 문제의식을 가지고 의료법윤리학에 입문하였습니다. 이러한 고민은 신중함을 요구하므로 그 진보가 더디게 이루어진 듯합니다. 하지만 그 시간은 필요한 것이었습니다. 연세대학교 의료법윤리학 박사과정의 수업 한 시간 한 시간이 모두 귀한 밑거름이 되어 이제 서로 다른 현상들로부터 조금은 정연한 일관성을 찾아 낼 수 있는 시각을 갖게 되었습니다. 후속 연구와 체계적이고 균형 잡힌 정보의 활용에 이 글이 한 줄이라도 도움이 되길 간절히 바랍니다.

2014년 12월

박미정 올림

차 례

그림 차례

표 차례

국 문 요 약

공공정보의 이차 활용을 위한 법제도에 관한 연구
- 생체·의료정보의 이차 활용을 중심으로 -

본 논문은 공공기관이 보유·관리하는 생체 및 의료정보의 이차 활용을 위한 법제도의 개선방안에 관한 연구이다. 공공기관이 보유·관리하는 정보의 수집목적 외 이차 활용이 증가하고 있는 시대적 흐름에 주목하고, 이러한 새로운 흐름에 비추어 우리나라 법제도의 나아가야 할 방향을 고찰하였다. 법제도 개선의 당위성을 찾기 위하여 우선 사적 권리와 공익의 개념에 대해 정리한 후, 이에 기초하여 공공정보의 이차 활용과 민감한 개인정보의 보호 간의 균형점을 발견하고자 하였다. 그리고 이 균형의 원리를 바탕으로 민감정보인 생체·의료정보에 대한 개인정보자기결정권의 보호와 공익을 위한 이차 활용의 가능성을 고찰하였다.

개인정보자기결정권은 자신에 관한 정보의 흐름을 자율적으로 결정할 수 있는 사적 권리다. 우리나라는 개인정보처리과정에 동의를 구하는 절차를 두어 정보주체의 자기결정권을 보호한다. 현행법은 정보주체가 '동의'를 통해서 사적 권리를 행사하도록 하고 있는데, 동의가 있으면 원칙적으로 제한 없이 개인정보의 수집·이용·활용이 허용된다. 그러나 공익적 목적으로는 동의 없이도 활용할 수 있다. 이차 활용은 이렇게 정보처리과정마다 동의를 요구하는 것이 아니고 특별법에 근거하여 동의를 면제하는 방식이므로 자기결정권을 행사할 수 없는 문제점이 있다.

생체·의료정보와 같은 민감정보는 특별히 개인정보자기결정권을 더욱 강조하여 법에서는 원칙적으로 그 처리를 제한한다. 그리고 일반 개인정보와는 달리 서면

동의 면제가 되지 않는다. 하지만 현실적으로 공공기관이 수집·보관·관리하고 있는 대규모의 공공정보에는 의생명과학연구에 이차 활용되는 생체·의료정보가 포함되어있다. 그리고 이러한 공공 정보는 정보주체의 동의가 면제된 채 공동 이용될 수 있다. 정부는 공공정보에 포함되어 있는 개인정보까지도 공공재로서의 유용성을 들어 이차 활용의 요구에 적극적으로 제공하려고 하지만, 정부가 독단적으로 그 결정권을 행사하는 것은 무리가 있어 보인다. 공공정보는 여전히 개인의 정보이다.

공공정보의 이차 활용이 증가하면서 법제도가 마련되고 있으나, 동시에 정보주체의 인격적·사회적 사생활침해의 위험성 때문에 생체·의료정보의 활용으로 인한 정보주체의 프라이버시 침해를 우려하여 활용에 대한 반감은 여전하다. 생체·의료정보와 같은 민감정보는 대부분 의생명과학연구에 이차 활용된다. 연구에 이차 활용되는 민감정보는 사전(事前)에 서면 동의를 받아야 하지만, 기관심의위원회는 서면 동의 면제의 적격성을 심의·의결한다. '생명윤리 및 안전에 관한 법률'에 의하면, 의생명과학연구에 있어 이차 활용되는 생체·의료정보는 기관심의위원회의 승인에 의해 연구대상자에 대한 서면동의가 면제되어 연구자들은 개별적으로 서면동의를 받지 않고 이차 활용할 수 있다.

생체·의료정보를 정보주체의 동의 없이 이차 활용할 수 있는 조건 중 다른 하나는 비 식별화 조치이다. 비 식별화된 정보는 익명성을 보장할 수 있다고 보아 프라이버시를 보호하는 방법으로 각광받고 있다. 하지만 이차 활용을 통하여 익명화된 정보가 재식별되는 경우가 있다. 그러므로 익명성을 확보하기 위하여 여러 가지 익명화방법을 적용할 수 있는데, 이차 활용을 위하여서는 구체적인 익명화 방법으로 통일할 필요가 있다. 또한 생체·의료정보는 그 자체만으로 식별이 되는 정보가 포함되어 있다. 그리고 익명으로 수집할 수 없는 경우가 더 많다. 그러므로 신기술이나 새로운 정보통신시스템을 설계 할 때 익명화의 유효성에 관한 기술적 조치로서 미리 가명화 기술을 적용하는 방안을 강구할 필요가 있다.

이와 더불어 그 익명성의 보장을 위하여 기술적인 측면과 더불어 재식별 여부를 판단 과정이 필요할 것이다.

의생명과학연구를 위해 이차 활용되는 생체·의료정보는 정보주체가 알 수 없는 시기에 미래의 목적에 쓰일 수 있으므로 정보주체에게 동의를 강요하거나 정보이용자에게 무조건 프라이버시 보호에 대한 의무 이행을 부담시키는 것은 부당한 측면이 있다. 정보화 사회에서 공공기관이 수집·보유·관리하는 개인정보에 대하여 정보주체는 그 사적인 권리를 정부에 맡기고 있다고 볼 수 있다. 따라서 공공기관은 수탁자로서 여러 기관의 개인정보처리자들을 규제하는 공통의 규칙이 체계적으로 마련되어야 한다.

개인의 자율성 존중과 권리보호 없이는 공익실현을 생각할 수가 없다. 진정한 공익은 개인의 권리보호의 테두리 안에서 이루어진다. 즉 개인의 권리보호라는 토대 위에서만 개인의 권리를 넘어서는 전체의 이익 추구가 가능하다. 민감정보의 이차 활용에 대하여 정보 주체가 알고 있어야하며, 서면동의를 면제하는 경우에는 사후(事後)에라도 정보주체가 개인정보자기결정권을 행사할 수 있도록 하는 것이 비례의 원칙에 합치하는 방안일 것이다. 필요하다면 재동의 및 사후 동의를 이끌어내는 제도를 시행할 수 있도록 개인정보보호 감독기구는 이러한 규칙을 수행하는 구심점 역할을 하여야 할 것이다.

생체·의료정보를 공익 목적으로 이차 활용하기 위해서는 자기결정권을 제한하는데 필요한 공익성이 우선적으로 담보되어야 하며, 사후 동의방식이 보충적으로 필요할 것이다. 만약 실정법의 해석만으로 공익의 실체적 내용을 확인할 수 없는 경우, 공익결정과정을 통하여 사적 권리와 공익을 균형 있게 고려하였는지를 심의할 필요가 있다. 이차 활용에 따른 익명성 보전을 위해서 사전 정보처리 및 이차 활용 후의 익명성에 대한 판단을 위해 전문가가 개입하는 방안이 마련되어야 할 것이다. 이를 위하여 공공기관이 생체·의료정보를 안전하게 공유하기

위하여 우선 필요한 각 공공기관 간 구속력 있는 규칙을 제시해보았다. 끝으로 민감정보를 수집하기 전 시스템 설계단계에서부터 프라이버시 보호의 개념을 포함시키는 방안을 제안하였다.

공공정보의 이차 활용이라는 새로운 국면에서 이차 활용을 위한 공익성의 합의과정과 익명성을 보전하기 위한 절차와 규칙, 그리고 법제도를 투명하게 운영하는 개선방향을 제안하여 민감정보의 이차 활용과 보호의 균형을 달성하고자 시도하였다.

핵심 되는 말 : 공공정보, 이차 활용, 정보프라이버시, 개인정보, 익명화, 개인정보보호정책, 민감정보, 개인정보보호기구, 바이오뱅크.

제1장 서 론

오늘날 많은 국가가 행정의 효율성과 투명성을 명분으로 전자정부의 구축에 힘을 쏟고, 사회의 모든 영역에 걸쳐 공공정보의 활용에 의한 막대한 부가가치 창출에 관심을 가지고 있다. 그리고 공공정보의 이차 활용을 위해 법제도를 개편하고 있다. 본 논문은 공공기관이 보유·관리하는 정보가 수집목적 이외로 활용되는 이차 활용이라는 새로운 시대적 흐름에 주목하고, 이러한 흐름에 비추어 우리나라 법제도의 당위성을 고찰하려고 한다. 연구배경, 연구목적, 연구방법은 다음과 같다.

1.1 연구배경

박근혜 정부의 '정부 3.0' 패러다임은 정부가 보유하고 있는 공공정보를 적극적으로 개방하고 공유하는 것이다. 공공정보 이차 활용이란 공공기관이 법령 등에서 정하는 목적을 위하여 생성 또는 취득하여 관리하고 있는 전자적 방식으로 처리된 자료 또는 정보를 목적 외로 활용하는 것을 말한다.

그동안 사회보장정책, 범죄, 교육, 치안, 세무, 학술연구 등 다양한 분야에서 공공정보의 이차 활용은 꾸준히 요구되었고, 이러한 요구를 충족시킬 수 있을 만큼 법적 근거가 만들어졌다.

우리나라는 1998년 제정된 '공공기관의 정보공개에 관한 법률'에서 처음으로 공공정보의 열람이나 기관간의 정보공유에 대해 규율하기 시작했다. 하지만 공공정보를 활용하고자 하는 수요가 적지 않음에도 불구하고 막상 공공정보의 활용은 부진하였다. '공공기관의 정보공개에 관한 법률'은 공공정보의 '제공'에 관한

법률이다. 즉 제공받은 공공정보의 '이용 및 활용'에 대해서는 아무런 규정을 두고 있지 않았다. 그 후 2010년 행정정보의 공동이용을 핵심내용으로 하는 개정 '전자정부법'이 시행된 이래, 공공정보의 이용은 꾸준히 증가하여 공공정보를 공동이용한 건수는 2011년 일억 건을 넘어선 것으로 나타났다(그림 1).[1)]

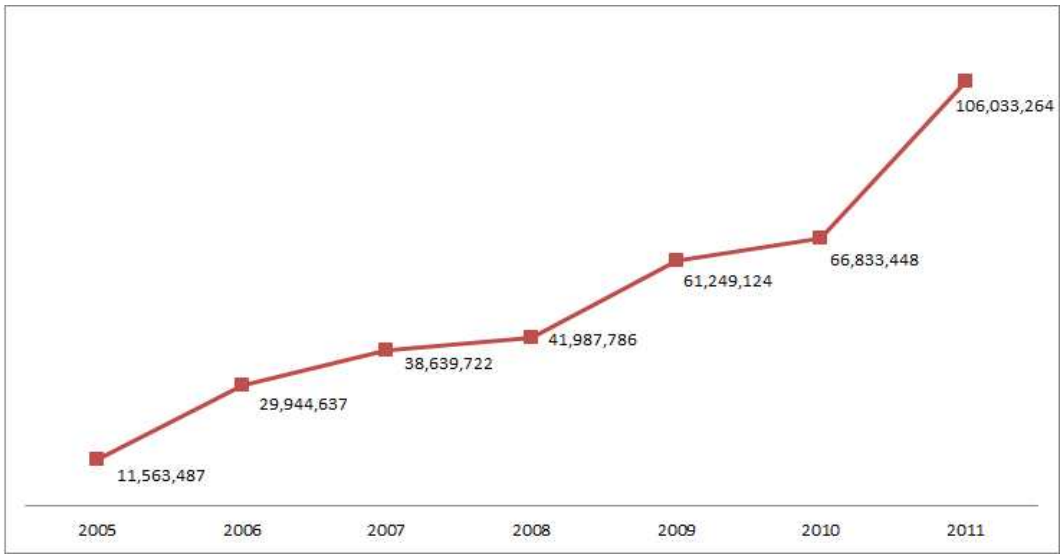

그림 1. 공공정보 공동이용 건수

공동이용의 결과로서 2011년 11월 기준으로 전 공공기관에서 1,612개의 민원사무 처리 시 120종의 구비서류가 불필요하게 되었다. 비용으로 보면 2012년 5월 기준 약 3억 9천만건의 공동이용을 통하여 약 1조 4천억 원에 달하는 사회적 비용을 절감한 것으로 평가된다.[2)]

---

1) e-나라지표에서 행정정보 공동이용 건수를 발췌하여 재구성하였다.
http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1025

2) 윤광석, 2012, "행정정보공동이용제도의 개선방안에 관한 연구", 정보화정책 제19권 제4호: 83-104면.

미국에서는 공공정보가 적극적으로 공개되었던 계기를 현실적·법률적·정책적 이유가 복합적으로 작용한 결과라고 평가한다.[3] 공공정보의 개방은 적극적이고 능동적인 시민들의 참여와 전문가 그룹 그리고 정부조직이 정보통신기술을 매개로 하여 새로운 생태계를 만들어나가는 차원에서 바라볼 수 있다. 국내에서도 2013년 '공공데이터의 제공 및 이용활성화에 관한 법률' 제정을 통하여, 공공기관 간 정보이용을 보편적으로 확대하기 위하여 필요한 제도적 기반을 마련하였다.[4] 그리고 동법은 다른 법률에 특별한 규정이 있는 경우를 제외하고는 우선 적용되는 특별법이다.[5] 그러나 이러한 공공정보에는 개인정보가 포함되어 있기 때문에, 비록 공공기관이 법률적 근거에 의해 이차 활용을 할 수 있다고 해도 정보주체의 프라이버시[6] 침해에 대한 법적 보호체계가 무엇보다 중요하다고 할 수 있다.

'개인정보보호법'에서는 개인정보를 일차 목적을 위해 수집할 경우에 개인을 식별할 수 없도록 하는 익명화 조치와 정보주체의 사전 동의를 통하여 정보프라이버시를 보호한다. 그러나 공공기관이 수집·보유하고 있는 생체·의료정보와 같은 민감정보의 이차 활용에 있어서도 마찬가지로 일차 활용에서의 정보프라이버시 보호방법인 익명화와 정보주체의 사전 동의만으로 개인의 권익을 보호할 수 있는

---

3) 선거 전략에 인터넷을 효과적으로 이용하였던 미국 오바마 대통령은 취임 직후 행정명령을 통해 참여와 협업을 위한 시스템 구축을 시도하였다. 그 후 예산관리처(Office of Management and Budget)는 행정명령인 이른 바 Open Government 명령을 발령하였고, 이에 따라 공공데이터를 공개하는 포털사이트인 data.gov가 구축·운영되고 있다. EXECUTIVE OFFICE OF THE PRESIDENT OFFICE OF MANAGEMENT AND BUDGET, 2009, 'Memorandum for the Heads of Executive Departments and Agencies on Transparency and Open Government', WASHINGTON, D.C..

4) 공공데이터의 제공 및 이용 활성화에 관한 법률 제3조 제1항.

5) 공공데이터의 제공 및 이용 활성화에 관한 법률 제4조.

6) 프라이버시(privacy)라는 말은 "사람의 눈을 피한다"라는 의미의 라틴어 'privatue'에서 유래하였고, 원래 사생활의 영역에서 파생되는 각종의 사실로서 타인에게 노출되지 않은 상태를 의미하였다고 한다. 권영성, 1983, "사생활권의 의의와 역사적 변천", 언론중재 여름호: 14면.

지에 관한 반성적 고찰이 필요하다.

이차 활용은 일차 수집 과정에서 익명화를 거친 정보를 활용하는 것이지만, 대부분의 경우 다양한 분야의 공공정보를 함께 활용하기 때문에 이차 활용과정에서 개인식별자가 다시 식별될 수 있는 위험성, 정보주체가 일차 수집에서 동의하지 않은 목적으로 개인 정보가 무단으로 활용될 수 있는 위험성, 민감한 정보가 일차 수집 과정에서 동의하지 않은 불분명한 목적을 위해서도 활용될 수 있는 위험성이 내포되어 있다. 그래서 이차 활용은 언제나 그 위험성을 줄일 수 있는 방안을 동시에 고려해야한다. 비록 공익을 위하여 공공정보를 이차 활용한다고 할지라도 사적 권리가 보장되지 않는다면, 사적 권리에 관한 분쟁의 발생으로 말미암아 공익을 위한 이차 활용 자체가 불가능해 질 수 있기 때문이다.

한편, 특별히 공공기관이 수집·관리하고 있는 정보 중에서 생체·의료정보는 법적 근거에 의하여 검사 및 치료 후, 일차로 수집·관리하지만 의료기관에서 공공기관으로 이전되면 그 성격은 공공정보가 된다. 예컨대, 진료비에 대한 심사·평가를 위한 진료비청구명세서는 의료기관에서 의료행위에서 얻어진 의료정보이나 건강보험심사평가원에서 보유·관리되고 있는 정보는 공공정보라고 할 수 있다. 그리고 이 공공정보는 대부분 의생명과학연구라는 특정한 목적을 위하여 이차 활용된다. 그런데 건강에 관한 정보는 정보주체의 사생활을 현저히 침해할 우려가 있는 민감한 개인정보로서 그 보호정도를 달리하고 있다.

이들 민감한 정보를 이차 활용하기 위해서는 충분한 설명에 근거한 서면동의가 필요하다. 하지만 정보주체에게 미래의 연구목적에 대해 충분히 설명하기도 어려울 뿐만 아니라 정보주체가 합리적 근거에 기초하여 동의를 할 만큼 이해하기도 힘들다. 또한 애써 익명화를 하였지만 필요에 따라 개인식별성 복원이 공공기관이나 연구담당자들에 의해 요청되기도 한다. 따라서 이러한 민감정보의 이차 활용을 위해서는 일반적인 공공정보를 이차 활용할 때와는 달리 특별한

조건과 특수한 원칙들이 필요하다.

일반적으로 민감정보는 인격적·경제적 이해관계를 가질 수 있기 때문에 실명화(實名化)되었을 경우, 기본적 인권이 침해될 가능성이 더 많은 특징을 갖는다. 이러한 정보들은 원칙적으로 제3자에 의한 처리 자체가 제한된다. 예외를 적용하려면 개인을 식별할 수 없도록 익명화 기술을 적용하거나 정보주체의 동의가 필요하다. 그러나 공공기관 간에는 정보주체의 동의 없이, 목적 외로 사용할 수 있는 법적 근거가 있다.[7] 이러한 이유로 자연스럽게 이들 민감한 정보의 이차 활용은 다양한 이해집단들 사이에서 끊임없이 논란의 대상이 되었고, 법적용에 있어서 혼란을 야기해 왔다.

공공정보의 이차 활용, 무엇보다 생체·의료정보의 이차 활용과 관련한 지금까지의 연구는 법학계에서의 개인정보보호, 보건학계에서의 학술연구를 위한 정보공개, 정보학계에서의 시스템보안 등의 관점에서 상당한 진전이 있었다. 그러나 이러한 연구들은 다소 분절적인 방식으로 수행되어 왔다. 따라서 이들 영역의 연구관점을 발전적으로 종합하여 다학제적 연구를 진행하고, 이에 기초하여 공공정보의 이차 활용과 민감한 개인정보의 보호 간의 균형점을 발견하고자 한다. 그리하여 이를 바탕으로 바람직한 법제개선의 방향으로 제시하고자 함이 본 연구의 출발점이자 배경이다.

1.2 연구목적 및 연구내용

본 연구는 공공정보에 포함되어 있는 생체·의료정보와 같은 민감정보가 이차 활용될 때 발생할 수 있는 프라이버시 침해 문제를 분석하여, 개인의 권리보호와

7) 전자정부법 제36조, 제38조; 공공데이터의 제공 및 이용활성화에 관한 법률 제4조, 제17조; 공공기관의 정보공개에 관한 법률 제4조; 개인정보보호법 제4조, 제5조, 제18조, 제23조; 보건의료기술진흥법 제26조 참조.

공익추구 간 균형의 원리를 도출하고, 이에 비추어 공공정보의 이차 활용을 위한 법제도의 당위성과 개선의 방향성을 밝히는 것을 목적으로 한다.

2장에서는 사적 권리와 공익에 관하여 그 법적 개념을 파악하여 두 개념의 긴장관계에 대해서 살펴본다. 공공정보 중 생체·의료정보의 이차 활용에 있어 특히 염려되는 문제는 정보주체의 자율성과 관련된 사적 이익과 정치적 공동체가 지향하는 공익이라는 가치의 충돌로 간주될 수 있다. 따라서 왜 이 두 개념이 균형을 이루어야 하는지에 대한 그 이론적 근거를 우선 도출하는 것이 민감정보일지라도 이차 활용을 할 수 있다는 법제도 개선의 방향성을 마련하는 토대가 될 것이다.

3장에서는 공공정보의 이차 활용의 문제점을 정보의 유용성과 프라이버시 침해와의 긴장관계 속에서 규명하고자 한다. 정보화 사회에서 공공기관이 수집·보유·관리하는 개인정보에 대하여 정보주체는 그 사적인 권리를 정부에 맡기고 있다고 볼 수 있다. 하지만 여전히 공공재로서 공공정보를 제공하고 이차 활용을 허용한다. 그러나 한편, 이러한 경우에도 여전히 공공정보에는 개인정보가 포함될 수 있기 때문에 정보주체의 프라이버시 보호를 간과해서는 안 된다는 측면에서 살펴본다.

4장에서는 공공기관이 수집·보유·관리하고 있는 생체·의료정보의 이차 활용을 가능케 하는 기술적·법제도적 측면의 쟁점 사항을 분석하고자 한다. 생체·의료정보와 같은 민감정보는 '개인정보보호법'을 근거로 하여 보호한다. 하지만 동 법률에 따르면 다른 법률에 특별한 규정이 있는 경우에는 공공기관은 개인정보를 목적 외로 이용·제공 할 수 있다. 그러나 이러한 정보를 이차 활용하는데 적용하는 법률은 '생명윤리 및 안전에 관한 법률'로서 정보주체의 서면동의를 통해 프라이버시를 보호하고 있다. 동시에 연구를 심의하는 기관윤리위원회에 연구의 적격성여부를 일임하고 있다. 현실적으로 양자가 함께 작용하는 국면에는 이차 활용대상 정보에 대한 동의부분에서 수범자에게 혼란을 야기하는 측면이

있다고 할 수 있다. 또한 여러 공공기관에서 제공되는 다양한 생체·의료정보가 링크되면서 이루어지는 이차 활용은 익명성 보전에도 한계가 있어 보인다. 의생명과학 연구 등의 목적을 위한 이차 활용과 생체·의료정보가 가진 특수성을 감안한 보호측면에서 법제도적인 정합성에 흠결이 있는지를 살펴본다.

5장에서는 생체·의료정보의 이차 활용도 저해하고 정보주체의 프라이버시도 보호하지 못하는 현행 법률체계에서 불완전성을 개선해 보고자 국제기구 및 외국의 민감정보 보호 방안과 이차 활용 방안을 비교하여 개선방안을 도출해 본다. 본 논문은 미국식과 유럽식의 입법체계를 비교의 기준으로 삼았다. 즉 시장중심적인 정책을 취하여 당사자들의 자율적인 규제에 맡기거나 필요한 경우, 분야별 입법에 의해 대체하는 미국식과 일반법으로서의 공통된 개인정보보호법을 두면서도 분야별 입법에 의해 미비점을 보완하는 유럽공동체의 방식을 주로 비교한다. 그리고 국제기구의 다양한 원칙들이 어떻게 개별국가에 입법기준이 되었는지도 함께 살펴본다.

6장에서는 공공기관이 수집·관리하고 있는 생체·의료정보를 이차 활용하는 과정에서 사적 권리와 공익의 균형점을 찾아야 한다는 연구 성과를 종합하여 규제적 요소와 기술적 요소를 포괄하여, 구체적인 개선방안을 제언하고자 한다.

1.3 연구방법

연구방법으로는 문헌고찰을 주로 활용하였으며, 특히 법제도 비교에 주안점을 두었다. 문헌고찰을 통하여, 우선 개인정보의 사적 보호와 공적 활용 간의 균형점을 이론적으로 탐색하고, 개인정보자기결정권[8] 제한의 한계에 대하여 고찰하였다.

---

8) 국내에서는 개인정보의 보호와 관련하여 개인정보자기결정권(권영성, 2002, 헌법학원론, 법문사: 422면 이하), 자기정보통제권(최대권, 2002, 헌법학강의, 서울, 박영사: 261-262면), 자기정보에 대한 통제권(성낙인, 2008, 헌법학 제6판, 파주, 법문사: 574-578면), 자기정보결정권(홍정선,

이러한 연구관심에 기초하여, 공공정보의 이차 활용 현황과 근거를 우리나라와 외국 각국 그리고 국제기구의 입법례에서 찾아 분석하였다.

외국법제에서 언급하는 개인정보보호 처리기술로서 익명화와 관련된 사안으로는 개인식별자 처리와 개인정보관리자의 역할, 시스템디자인에 대한 문제를 주된 연구대상으로 삼았다. 공공정보의 이차 활용은 제3자에게 전송된 정보를 활용하는 것이 대부분이라는 점을 인식하고 국제기구에서 정보 이전을 위한 안전조치로서 활용하는 구속력 있는 규범들을 비교하여 우리나라에 적용 가능한 공통된 사항을 추출하였다.

한편, 연구의 적실성과 현실 적용성을 높이기 위하여 인터뷰에 기초한 연구방법론도 활용하였다. 공공정보 중에서 민감정보를 가지고 있는 공공기관의 실무자와의 면담을 통해 제공하는 입장에서의 애로 사항을 정리하고, 의료기관의 연구자등 민감정보를 이차 활용하는 의생명과학 연구 분야의 전문가와 면담을 통하여 정보의 이차 활용측면에서의 불만 사항을 청취하여 그 내용을 참고하였다.

또한, 이차 활용 및 개인정보 보호 실무를 파악하기 위하여 현장방문을 수행하였다. 개인정보보호와 관련된 감독 기구의 역할에 대한 개선방안을 찾고자 국내에서는 개인정보보호위원회의를 방청하였다.

외국에서는 프랑스의「국가정보처리자유위원회(Commission Nationale de l'Informatique et des Libertés, 이하 CNIL)」가 다른 국가들의 감독기구와 비교해서 가장 독립적이고 정보보호를 위한 다양한 권한을 갖고 있다는 선행연구[9]에 기초하여

2012, 행정법원론(상), 서울, 박영사: 563-567면) 등 다양한 용어가 사용되고 있다. 본 논문에서는 '자신에 관한 정보의 흐름을 스스로 결정하거나 자율적으로 통제할 수 있는 권리'로 이해하여 개인정보자기결정권이라는 용어를 선택한다.

9) 이광윤 외, 2009, 공공부문의 개인정보 활용·공개 및 보호에 관한 법제 연구 - 프랑스, 독일, 영국, 일본을 중심으로-, 한국정보보호진흥원: 5-81면; 정재황, 2006, "프랑스법에서의 개인정보의 보호에 관한 연구" 공법연구 제34집 제4호 제1권: 251-286면; 이한주, 2013, "개인정보보호위원회 제도의 문제점과 개선방안 -프랑스 CNIL과의 비교를 통하여-", 경북대학교 법학논고 제41집: 477-500면; Fenoll-Trousseau et G. Haas, 2000, "Internet et protection des donnés personnelles", Litec, Paris: p. 96.

직접 이곳을 방문하여 건강국의 법무팀, 유럽국제팀 책임자와 인터뷰하였다. 또한 이들로부터 공공정보의 이차 활용을 전담하는「공공기관의 행정문서에 대한 액세스 위원회 (La Commission d'accès aux documents administratifs, 이하 CADA)」에 대한 소개를 받아 해당 부서와 이메일로 교신하였다.

각국의 주요 공공기관 공식 홈페이지와 바이오뱅크 포털 사이트를 방문하여 실제적인 현황 파악을 하고, 실무자와 이메일을 통해 질의응답을 교환하고 그 내용을 참고하였다. 이러한 연구방법을 종합하여 그림 2와 같이 제시한다.

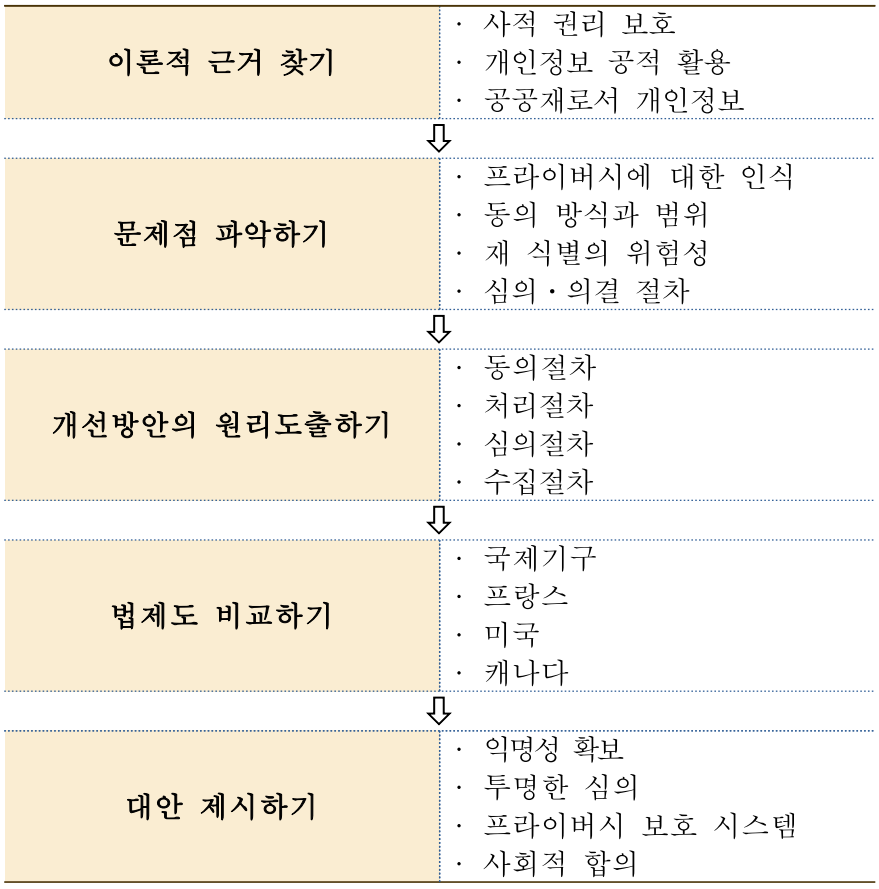

그림 2. 연구의 틀

제2장 개인정보의 사적 보호와 공적 활용

본 연구의 주된 분석대상인 생체·의료정보는 사적인 영역에서는 비밀스럽게 보호되어야 할 대상이지만, 공적인 영역에서는 어떤 특수한 목적을 위하여 활용하도록 허용할 수도 있는 양면성을 갖는다. 본 논문은 이러한 개인정보가 갖는 두 가지 성격 간에 충돌이 발생할 수 있으며, 그 경우 균형의 원리에 입각하여 그러한 갈등을 해소하고 조화를 모색하는 것이 바람직한 법제개선의 방향이라는 전제로부터 출발한다. 제2장에서는 현대 정보화 사회에서 개인정보가 갖는 이중적 성격을 검토하고, 개인정보의 사적 보호필요성과 공적 활용필요성 각각을 확인한 후, 균형의 원리에 입각하여 양자 간 조화필요성을 제언하는 이론적 고찰을 수행한다.

2.1 개인정보의 이중적 성격

오늘날 정보통신기술의 발달과 정보의 활용 능력은 국가사회 시스템운영의 효율성에 중대한 영향력 미치는 요인이 되었다. 그래서 개인과는 별개로 존재하는 개인정보일지라도 그 정보 주체는 항상적 감시 내지는 통제에 놓일 수 있다는 우려를 갖게 되고, 타인이 나의 정체성을 결정할지도 모른다는 염려를 하게 된다. 이러한 우려로 인해 개인정보가 어디에 어떻게 수집·보관되어 있든지, 원래의 목적에 부합하게 사용되고 있는지를 알고 통제할 수 있는 권리를 정보주체에게 보장해 주어야 한다는 주장이 등장한다. 이는 단순히 개인정보에 대한 소극적 침해배제나 적극적 접근 및 수정권의 보장을 넘어 정보주체의 자기정보결정권의 행사가 매우 중요하게 인식되는 사회적 변화라고 할 수 있다.

하지만 개인정보를 수집·관리하는 정보통신기술은 법 제·개정의 속도 보다

훨씬 빠른 흐름으로 변화하고 있다. 더욱이 정보를 모아 다양한 분야에서 이차 활용할 수 있는 가능성은 증가하고 있다. 이제 개인정보주체는 “자신의 개인정보가 어떻게 수집, 처리, 관리, 이용되는지에 대한 감독권”으로서 ‘개인정보자기결정권’을 이해하고, 이러한 통제권을 능동적으로 행사할 필요성이 있다.[10]

한편, 개인정보에는 정체성과 관련된 인격적 가치 이외에도 공적 활용에 동원될 수 있는 재산적 가치가 포함되어 있다. 따라서 개인정보의 이차 활용의 허용은 그 공공재적 성격에 비추어 마치 지적재산권에 있어서 ‘공정이용(fair use)’ 법리와 같이 그 수집·이용에 있어서 탄력성을 도모하는 법리구성이 필요하다는 주장도 설득력을 얻고 있다.[11] 헌법상 기본권으로서 ‘개인정보자기결정권’이 인격적 가치 보호 측면에서 개인정보의 보호에 중점을 두는 것이라면, 공공정보로서 개인정보의 이차 활용은 개인정보의 재산적 가치에 중점을 두는 것이라고 할 수 있기 때문이다.

2.2 사적 권리로서 개인정보보호의 필요성

2.2.1 정보프라이버시권론

사적 권리로서 개인정보 보호의 필요성을 검토하기 위해서 개인의 권리가 어떻게 사회적 맥락에서 보장될 수 있을지에 관한 웨스틴(A. F. Westin)의 통찰에 주목할 필요가 있다. 그는 ‘개인이나 단체 또는 기관이 스스로에 관하여 타인과 의사소통을 함에 있어서 그 시기, 방법과 정도를 결정할 수 있는 권리’로서 프라이버시권을 정의한다.[12] 그리고 중요한 것은 이러한 권리가 사회적인 관계를

10) 김종철, 2001, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 인터넷법률 제4호: 40-43면.

11) 로렌스 래식, 김정오 옮김, 2006, 코드 2.0, 서울, 나남: 451-458면.

설정한다는 것이다. 프라이버시권은 구체적으로 고립성(solitude), 친밀성(intimacy), 은닉성(reserve), 익명성(anonymity)이라는 성질로 구성된다.

'고립성(solitude)'은 평온하게 타인이나 공공으로부터 물리적으로 떨어져 있는 것을 의미한다. 이에 반해 친밀성(intimacy)은 둘 사이에서나 혹은 개인적으로 서로에 밀착하여 편안함과 솔직함을 느끼는 것으로서 부부관계, 가족관계, 친목회 등이 그 예이다.

'은닉성(reserve)'은 원치 않는 침해로부터 심리적 장애물을 설치하는 것을 말한다. 인간이 자신을 둘러싼 환경으로부터 자신에 대한 접근을 차단하는 한계를 설정하는 경우다. 인간의 삶은 대부분 어느 정도의 친밀성을 갖고 다른 사람과 연결되어 있게 마련이지만 아주 친밀한 관계라 할지라도 타인과 공유하지 않고 자신만 갖고 있고자 하는 부분이 있는 것이다. 지극히 사적인 것이거나 아주 성스러운 것, 치욕스런 것, 표현하기에 불경스런 것 등이 바로 그런 것이다. 이러한 은닉성의 요소 때문에 인간관계에서 '정신적 거리(mental distance)' 혹은 사회적 관계에서 '사회적 거리(social distance)'를 만들어 의사소통을 한다.

'익명성(anonymity)은 인간이 공적 영역에서 활동하게 되는 경우에 스스로의 정체를 밝히지 않고 감시받지 않는 상황에서의 자유로운 행동을 하고자 하는 경우에 필요한 것이다. 익명성의 긍정적인 측면을 강조하는 입장에서는 익명성이 개인에게 새로운 자아정체성을 발견하고 인간관계를 형성할 수 있는 기회를 제공한다고 주장한다.[13] 또한 익명성은 연령이나 성별 같은 사회적 정체성의 영향을 배제시킬 수 있는 수단이기 때문에 보다 평등한 상황을 설정할 수 있게 해준다.[14]

---

12) Alan F. Westin, 1970, Privacy and freedom (Vol. 67). New York: Atheneum. p. 7; "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

13) Elizabeth M. Reid, 1991, Electropolis: Communication and community on internet relay chat. Melbourne, University of Melbourne: pp.6-19.

웨스틴이 지적하는 프라이버시권으로서 정보프라이버시를 바라본다면, 개인정보자기결정권이라는 헌법적 권리는 단순히 인격적 가치의 보호 이상의 의미를 갖는다. 왜냐하면 그것이 개인의 존엄성, 자아정체성, 창조성, 자율성과 연결점을 형성함으로써, 헌법의 최고가치인 인간존엄과 자율성 내지 자유권의 핵심이념인 자기결정권의 근원적 전제를 형성하기 때문이다.

2.2.2 헌법상 기본권으로서 개인정보자기결정권

우리나라에서는 정보프라이버시권을 헌법상의 권리로서 '개인정보자기결정권'으로 파악한다. 헌법재판소는 다음과 같이 판시한 바 있다.[15]

> "개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정 할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다.
>
> 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다."

---

14) Joseph B. Walther & Judee K. Burgoon, 1992, "Relational communication in computer mediated interaction", Human communication research, 19(1): pp. 50-88.

15) 헌재 2005. 5. 26. 99헌마513, 주민등록법 제17조의8 등 위헌확인 등.

하지만 개인정보자기결정권의 헌법적 근거에 대해서는 견해가 갈리고 있다. 즉 사생활의 비밀과 자유(헌법 제17조)에서 찾는 학설도 있고[16], 행복추구권(헌법 제10조)의 한 내용으로 해석하는 학자도 있다.[17]

헌법 제17조는 사생활 영역에서 비밀과 자유를 보장한다. 여기서의 생활의 비밀은 자신의 의사에 반하는 사생활의 공개를 당하지 아니할 권리를 말한다. 그러나 자유의 개념과 보호범위, 법적 성격 등에 대해서 대립되는 견해가 나타나고 있으며, 자신에 관한 정보를 자율적으로 통제할 수 있는 권리가 사생활 보호에 포함되는지에 대해서도 다양한 견해가 제시되고 있다.[18]

성낙인 교수는 헌법 제17조 사생활의 비밀과 자유의 적극적인 측면으로 '자기정보통제권'을 이해할 수 있다고 한다.[19] 그래서 정보관리시스템을 설치할 때는 일정한 종류의 기록금지, 개인정보수집방법의 제한, 개인의 의사에 반한 입력금지, 개인정보의 무제한 축적의 금지, 자기파일에 대한 액세스권의 보장, 개인정보의 정정권의 보장, 남용금지 등이 요망되는데, 이러한 것들은 자기정보통제권의 중요한 내용이 된다고 한다.[20] 헌법재판소도 개인정보에 대한 사적 권리를 인격권으로서만이 아닌 청구권으로 해석하고 있다.[21]

---

16) 권영성, 2002, 헌법학원론, 서울, 법문사: 422면 이하 참조; 최대권, 1999, 헌법학강의. 서울, 박영사: 261-262면.

17) 김철수, 2000, 헌법학개론, 서울, 박영사: 522면 이하 참조.

18) 변재옥, 1991, "현대사회에 있어서 정보공개와 인권보장", 저스티스 24(2): 7-27면; 김일환, 2001, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 공법연구 29(3): 87-112면; 김종철, 2001, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론", 인터넷법률 4호: 23-44면. 강경근, 2005, "情報保護의 憲法規範的 接近과 展望", 공법학연구 6(2): 203-223면; 김용섭, 2001, "정보공개와 개인정보보호의 충돌과 조화", 공법연구 29(3): 167-199면.

19) 성낙인, 2008, 헌법학, 파주, 법문사: 574면 이하 참조.

20) 성낙인, 위의 책: 574-578면.

21) 대법원 1998. 7.4. 선고 96다42789 판결 참조; "우리나라 법률체계에서는 자신에 관한 정보를 공권력이 함부로 수집, 제공, 이용하지 못하도록 한다는 측면에서 자율권적 성격을 가진다고 할 수 있다. 그리고 개인이 단순한 정보의 객체로 전락하지 않도록 보장한다는 측면에서는 인격권적 성격도 가진다. 또한 기록된 개인정보가 부정확한 데서 초래되는 폐해를 방지하거나 적극적으로 오류를 정정할 수 있도록 한다는 점에서는 청구권적 성격도 가진다고 볼 수 있다."

김일환 교수는 '정보자기결정권'은 인간으로서의 존엄과 가치에 관련되는 내용이라 할 수 있겠으나 헌법 제10조에 대해 특별법적 성격을 가지는 제17조의 규율내용으로 보아도 무방할 것이라고 한다. 정보화 사회가 급속히 진행되는 오늘날, 헌법 제17조의 사생활 비밀과 자유는 사행활의 평온을 침해받지 아니하고 사생활의 비밀을 함부로 공개당하지 아니할 권리로서 자신에 관한 정보를 관리·통제할 수 있는 권리도 포함하는 것으로 이해된다는 것이다.[22]

이와 관련한 판례도 있다. 자신에 관한 정보를 스스로 관리, 통제 할 수 있는 권리가 인격권, 자유권의 일종이며, 이것이 정보화 사회에서는 정보프라이버시권이라는 판례이다.[23] 대법원 또한 헌법 제10조와 제17조를 적용하여 이른바 '개인정보자기결정권'이 보장된다고 판단한 바 있다.[24]

정리하면, 개인정보자기결정권은 사생활의 비밀과 자유를 보호할 뿐만 아니라, 개인정보가 갖는 인격적 가치로부터 파생되는 개인의 정체성과 인간의 존엄성을 보호하는 측면도 가지고 있다고 할 수 있다. 본 논문은 헌법 제10조 행복추구권의 핵심내용인 자기결정권과 헌법 제17조의 사생활의 비밀과 자유 보장 양자 모두를 종합하여 개인정보자기결정권의 근거 내지 성격을 결정하여야 한다고 본다. 더 나아가, 아래에서 검토하는 바와 같이 개인정보의 공공재적 성격으로 인해서 그 제공과 제공에 따른 편익의 선택권 또한 개인에게 주어져야 한다고 본다.

---

22) 김일환, 앞의 논문(주 17): 101-102면 참조.

23) 서울고등법원 1995. 8. 24. 선고 94구39262 판결. 하집 1995(2)464 참조: "사생활의 비밀과 자유의 불가침은 사생활의 내용을 공개당하지 아니할 권리, 사생활의 자유로운 형성과 전개를 방해받지 아니할 권리, 그리고 자신에 관한 정보를 스스로 관리 통제할 수 있는 권리 등을 내용으로 하는 권리로서 인격권 자유권의 일종인데 오늘날 정보화 사회가 급속히 진행되면서 그 보고가 절실하여 이를 국가가 보호하여 주지 아니하는 경우 기본권이 바로 침해를 받는 직접적 권리다."

24) 대법원 1998. 7. 24. 선고 96다 42789 판결: "헌법 제 10조와 제 17조의 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다."

2.3 공공재로서 개인정보 활용의 필요성

현대사회에서 개인은 자신의 개인정보를 제공하고, 그로부터 일정한 혜택을 받는 일종의 교환(trade-off) 관계를 형성한다. 예컨대, 공적 영역에서는 개인정보를 제공하고, 시민권을 인정받고, 선거권, 사회보장수급권 등 권리와 혜택을 누린다. 사적 영역에서는 개인정보를 제공하고, 맞춤형서비스(customized service)를 제공받기도 한다.

특히 오늘날 공공정보로서 개인정보의 제공과 활용을 통한 경제적 부가가치의 창출이 새삼 주목받고 있다. 예컨대 현 정부에서 천명한 정부 3.0은 공공정보의 가치를 '공공정보를 적극 개방·공유' 하여 '국민 맞춤형 서비스를 제공'하려는 행정서비스의 혁신을 위한 토대로 두고 있다. 공공정보의 개방은 공공부문과 시민생활과 밀접하게 연결되어 있고, 나아가 민간경제에 도움을 줄 수 있다. 2011년 기준 생산유발액은 23조 9천억 원, 부가가치유발액은 10조 7천억 원, 고용유발인원은 14만 7천명으로 추산된다.[25)]

공공정보를 활용하여 수요자맞춤형 서비스를 발굴하려는 시도는 여러 공공기관의 다양한 공공정보가 사회·경제적 지표로서 함께 이차 활용된다는 것을 반증한다. 여러 공공기관의 정보를 통합하여 분석한 결과가 현황을 파악하여 보다 적절한 해석을 하는데 타당성을 높이고, 이 결과가 전문가는 물론 일반인에게도 신뢰감을 주기 때문이다.

공공정보는 교통, 환경, 교육, 에너지, 실업문제 등 국민생활과 삶의 질에 직접적인 영향을 미치는 공적 문제들을 보다 효율적으로 해결하는데 활용된다.[26)] 이러한 정보들은 해당 분야에서도 유용하지만, 다른 분야의 정보와 함께 활용될 때, 그 유용성이 배가된다. OECD는 공공부문의 정보(Public Sector information, PSI)를

25) 이승재, 2013, "정부 3.0과 공공데이터 개방전략", 한국지역정보개발원: 1-6면 참조.
26) 공공데이터의 제공 및 이용활성화에 관한법률 제1조.

활용할 수 있는 분야와 유형별 이차 활용 데이터를 다음과 표 1과 같이 제시한 바 있다.[27]

표 1. 공공부문 이차 활용 데이터

분 야	유 형
사회복지	인구통계학적 정보 (demographic data)
	건강관련 정보 (data on health/illness)
	교육 및 근로 정보 (education and labor statistics)
교통 및 운송	운송정보 (transport network)
	교통정보 (traffic information)
	운송 통계 (transport statistics)
	자동차 등록정보 (car registration data)
여행 및 레저	호텔정보 (hotel information)
	여행객 통계 (tourism statistics)
농업, 수산, 식품	토지이용 정보 (cropping/land use data)
	농업 소득 정보 (farm incomes/use of resources)
	어류 및 양식장 정보 (fish farming/harvest information)
	가축 정보 (livestock data)
자연 및 환경	생태정보 (biologic and ecologic information)
	에너지 자원 및 소비 정보 (energy resource/consumption information)
	지질 및 지구물리학정보 (geological and geophysical information)
사법	범죄 기록 (crime/conviction data)
	사법판결 정보 (information on legislation)
	특허 및 상표 정보 (patent and trademark information)
산업, 경제	재무 정보 (financial information)
	회사 정보 (company information)
환경	기상 정보 (meteorological data)
	대기 정보 (atmospheric data)
국토 및 지리	지도 제작 정보 (cartographic information)
	공간, 지리적 좌표 (spatial data/geographical coordinates)
	지형정보 (topographical information)
	토지이용정보 (land use info (cadastral data)
과학	대학 연구정보 (university research)
	공적 자금 출연 연구정보 (publicly-funded institutes research)
	정부 출연 연구정부 (governmental research)
교육	학술 논문 정보 (academic papers)
정책	선거정보 (governmental election)
	지자체 및 중앙정부 행정소송정보 (local and national proceedings of governments)

27) OECD, 2006, “Digital broadband content: public sector information”, OECD Digital Economy Papers, No. 112, OECD Publishing: pp.1-83.

2013년 통계청에서 실시한 사회조사설문에서는 국민이 향후 가장 필요한 복지로서 '건강관리·증진서비스'가 선택되었다(39.4%).[28] 보건의료계에서는 환자 중심의 자기건강관리는 전략적 과제로 간주하고, 이를 실현하는 방법으로서 건강관련 데이터 분석을 그 토대로 삼는다. 특히 각 의료기관이 의료 정보화를 위해 도입한 임상의료 정보시스템, 임상연구 지원시스템 등을 통하여 데이터 웨어하우스에 집적된 질병치료관련 정보는 임상연구영역에서 그 활용도가 높아졌다.

직접적인 진료정보 이외에도 진료정보가 포함되어있는 행정정보도 연구에는 유용하다. DNA와 의료정보를 연계하여 약물과 치료기법을 개발하는 등의 학술연구는 질병관리본부나 건강보험심사평가원, 암센터와 같은 공공기관의 정보를 필요로 한다. 재난 전조를 감지해서 대비체계를 구축한다거나, 감염병 발생 경로들을 예측하여 사전 예방 및 통제 시스템을 갖춘다거나, 질병의 예방·감시·관리를 보다 효율적으로 하기 위한 연구에서 이러한 공공기관의 정보는 더욱 유용하다. 공중보건 등 공익의 목적이므로 그 활용의 정당성을 찾을 수 있지만 공공정보에는 개인정보가 포함되어 있다는 것이 문제가 된다. 따라서 공공정보의 활용에 대한 쟁점은 개인정보 수집·관리·이용 그 자체가 아니라, 어떤 목적으로 누가, 어떠한 수준에서 활용하는지에 대한 것으로서 공공정보에 포함된 개인정보주체의 참여권 내지 통제권의 보장 여부라고 할 수 있다.

정보주체의 개인정보자기결정권을 참여권이나 통제권으로 해석하면, 개인정보의 보호와 개인정보의 공적 목적의 활용 간에 빚어지는 충돌을 해결할 실마리도 그러한 참여 내지 통제에서 발견할 수 있다. 또한 공공재로서 개인정보를 활용하고 보호하는데 미흡한 현행 법률체계의 흠결을 보완하는데 있어서 고려해야 할 원리로서 활용과 보호, 양자 간의 균형점을 찾을 필요성을 높인다.

---

28) 2013년 사회조사 결과, 2013. 통계청.

2.4 사적 보호와 공적 활용 간 균형의 원리

사적 권리의 행사와 공공성은 갈등을 빚는다. 개인은 여러 사회적 관계 속에서 상호적인 상황에 놓인 주체들이다.[29] 그래서 법을 적용하기 이전에 이미 수많은 상이한 가치들 속에서 균형을 잡아야 하고, 때로는 상충하는 여러 원칙들 속에서도 통합을 이루어야 한다.[30] 개인정보의 보호와 개인정보의 공적 활용도 마찬가지라고 할 수 있다.

2.4.1 공익의 구성적 측면

공익(public interest)이라는 개념을 표현하는 용어는 나라마다 조금씩 차이가 있다. 프랑스에서는 개별이익에 대립되는 의미로 '일반이익'이라는 개념이 주로 사용된다. 반면, 미국에서는 개인이 획득하려고 하는 모든 영역의 재화로서 '공공선(public good)'과 '공익'을 구분하지 않고 사용한다.[31] 또한 '국민 모두 또는 공동체 주민 모두에게 혜택이 돌아가는 이익(interest to all the members of the public)'으로 정의하기도 한다.[32] 이러한 상이함에도 불구하고 프랑스와 미국에서 사용되는 공익개념은 공동체의 가치를 포함하고 있다고 볼 수 있다.

국내에서 공익 개념에 대한 심도 있는 연구는 많다.[33] 김 도균 교수는 우리

---

29) 김정오 외, 2012, 법철학, 서울, 박영사: 184-186면.

30) Baruch A. Brody, 1988, The Ethics of Biomedical Research: An International Perspective, Oxford, Oxford University Press: p. 205.

31) Albert O. Hirschman, 1992, Rival Views of Market Society and Other Recent Essays, Cambridge MA, Harvard University Press: pp. 35-55.

32) Lain McLean & Alistair McMillan, 2009, The concise Oxford dictionary of politics, Oxford, Oxford University Press.

33) 김도균, 2006, "법 원리로서의 공익 -자유공화주의 공익관의 시각에서-", 서울대 법학, 제47권 제3호: 155-215면; 박균성, 2006, "프랑스 행정법상 공익개념", 서울대 법학, 제47권 제3호:

나라의 현행 헌법에서 가장 대표적인 공익의 개념을 공공질서유지와 관련된 것들로 보고 있다.[34] 예를 들면, '국가의 독립, 영토의 보전·국가의 계속성·헌법수호'(제66조), '국가안전보장과 질서유지'(제23조 2항, 제37조 2항), '공공의 안녕질서'(제76조 1항, 제77조 1항), '국가의 안녕질서'(제109조), '선량한 풍속'(제109조)과 같은 표현들이 그것이다. 또한 '공중도덕이나 사회윤리'(제21조 4항), '공공복리'(제23조 2항, 제37조 2항), '공공필요'(제23조 3항), '주민의 복리'(제117조)를 공익으로 보고 있다. 그리고 '환경보전'(제35조), '국토의 효율적이고 균형 있는 이용·개발과 보전'(제122조), '국민경제상 긴절(緊切)한 필요'(제126조), '국민경제의 발전'(제127조)과 같은 조항에서도 공익의 개념을 찾을 수 있다고 한다.[35]

헌법 이외의 실정법 분야에서도 공익 개념은 다양하게 사용되고 있다. 입법목적으로서, 규제정책목표로서, 개인의 자유를 제한하는 근거로서, 인허가의 근거로서, 사정변경의 근거로서, 그리고 하위법령에서 구체화되어야 할 전제로서 다양하게 사용된다. 공익의 개념은 이렇듯 개인과 사회의 관계를 어떻게 이해할 것인가라는 것과 밀접하게 관련되어 있다.

한편, 공익 개념 구성과정과 공익 판단과정을 실천적 논의의 과정으로 접근할 필요가 있다. 이 과정을 통하여 상대방과 공중이 납득할 만한 근거를 제시하고 입증하여 그 과정의 결과 위에 공익의 개념을 구축하는 것이다. 이러한 관점은 공익을 결정하는 주체들이 복수의 이해당사자들이나 집단일 수 있다는 것을 암시한다.

27-51면; 김유환, 2006, "영미에서의 공익개념과 공익의 법문제화 -행정법의 변화와 대응-" 서울대 법학, 제47권 제3호: 52-88면; 최송화, 1996, "행정법상 공익개념의 전개와 의의", 현대헌법학이론, 우제 이명구 박사 회갑 기념논문집(II), 서울, 고시연구사: 89-113면; 최송화, 2000, "공익개념의 법문제화: 행정법적 문제로서의 공익", 서울대 법학, 제40권 제2호: 27-52면; 권형준, 2003, "정보통신의 발달과 헌법상의 과제", 한일법학 22: 85-114면; 이계만 외, 2011, "한국의 공익개념 연구: 공익관련 법률내용 분석을 중심으로", 한국정책과학학회보 15(2): 1-27면.

34) 김도균, 앞의 논문(주 32): 155-215면.

35) 최송화, 2002, 공익론: 공법적 연구, 서울, 서울대학교 출판부: 210-215면.

즉 어느 한 집단이 일방적으로 공익을 결정할 정도로 그 수단이 합리적이거나 실질적이지는 않지만 상호조정하거나 합의하여 공익을 결정할 수 있을 것으로 본다.

이러한 맥락에서 공익의 정당성을 찾는다면, 토론정치를 통하여 공익을 간주관적으로 생성된다는 입장을 취한 학자로서 하버마스(Jürgen Habermas)에 주목할 필요가 있다. 하버마스는 공익을 결정하는 자들을 시민 사회적 결사체로 보았다. 따라서 관료들은 시민들의 자유를 보장하고 토론절차를 확립하는 등 시민사회를 활성화시키는 역할을 수행해야 한다고 주장했다.[36] 그리고 이런 토론에 객관적으로 참여함으로써 참여자 스스로는 애초의 단순한 주관적 견해들을 극복하고, 이성적 동기에서 출발한 확신을 공통적으로 도출하여 각자의 삶과 연관시킬 수 있는 상호주관성을 확인할 수 있게 된다.[37]

이렇게 정치적 공동체의 근본가치들을 해석하는 과정에서 공익이 구성될 수 있다면, 공익의 내용에 대한 불일치는 단순히 주관적인 선호에 대한 불일치가 아니라 논의를 통해서 균형을 맞추는 시도를 할 수 있는 불일치임을 뜻한다.[38]

그렇다면, 어떤 정책이 적용될 상황들과 그 정책이 시행되어 개인들과 사회에 미칠 영향을 고려하여 공익판단을 할 수 있다는 이론적 출구는 될 수 있을 것이다. 그러므로 실정법의 해석만으로 공익의 실체에 대하여 확인할 수 없는 경우라면, 연구자는 '공익결정과정에 공평하게 참여할 기회를 보장받았는가'로서 사적 권리를 보장받았는지를 판단할 수 있다고 본다.

---

36) Jürgen Habermas. 1995, "Reconciliation Through the Public use of Reason: Remarks on John Rawls's Political Liberalism", The Journal of Philosophy, Vol.92, No.3, pp. 109-131.

37) Jürgen Habermas, Translated by Thomas Mccarthy, 1984, The theory of communication action. Boston, Beacon Press: pp. 85-101, 284-288.

38) 김도균, 앞의 논문(주 32): 155-215면.

2.4.2 공익 추구와 사적 권리 간 균형의 원리

공공재로서의 개인정보, 그 중에서도 생체·의료정보와 같은 민감한 정보의 공익을 위한 이차 활용이라는 긴장관계는 불가피해 보인다. 하지만 이러한 개인의 권리와 공익이 상충되는 긴장관계 속에서 당사자들의 의사소통은 매우 중요하며, 사적 권리의 실현은 공익을 추구하는 과정과 함께 다루어야 하는 문제임을 상기시켜 준다.

하버마스는 '포괄적 합리성'과 '절차적 합리성' 두 가지로 의사소통합리성을 설명한다. 포괄적 합리성은 상대방을 상호이해를 지향함에 있어 서로 협력해야하는 동반자로 간주한다.[39] 따라서 포괄적 합리성은 직접적인 목표를 관철하기 위한 도구로 축소되는 것을 비판하면서, 분화된 영역의 모든 측면을 해명할 수 있을 만큼 포괄적이어야 함을 강조한 것이라고 볼 수 있다.

한편, 절차적 합리성은 애초에 가졌던 개인적이고 주관적인 견해를 뛰어 넘어 이성적인 확신에 따라 자발적으로 상호이해와 합의에 이르도록 하는 것이다. 이러한 절차는 그 수행과정마다 타당성을 요구하면서 척도를 스스로 발견하기도 한다.[40] 동시에 다루어지는 문제의 내용상 차이에도 불구하고 그것의 해결을 위한 보편적 타당성이 바로 이 절차에서 마련되기도 한다. 이와 같이 분화된 영역에 대한 고려가 필요하고, 자발적인 상호이해가 중요하다는 점에서 공공정보의 이차활용을 위한 법제도의 정당성 확보를 위하여 포괄성과 절차성을 주된 특징으로 갖는 의사소통의 합리성을 이론 정립을 위해 간접적으로 활용하려고 한다.

전통적으로 공익은 의회의 입법과 행정의 집행, 그리고 법원의 재판을 통해

---

39) 선우현, 1998, "합리성이론으로서 하버마스의 비판적 사회이론", 서울대학교 대학원, 박사학위논문: 59면.

40) Jürgen Habermas, Translated by Frederick Lawrence, 1987, *Der Philosophische Diskurs der Moderne: Zwölf Vorlesungen,* Cambridge MA, MIT Press: pp. 330-366.

실체적으로 확정될 수 있는 것으로 인식되었다. 하지만 현대 산업사회와 같이 복잡해지고 다양한 가치사회에서, 공익은 실체적으로 확정될 수 있는 크기로 이미 존재하는 것이 아니라 절차를 통해 대립하는 다양한 이익들이 새롭게 출현하고 이를 형량·조정함으로써 비로소 정립되는 것으로 이해된다. 그리고 국가가 보장하는 참여기회와 절차는 시민 상호간의 이익조정 뿐만 아니라 국가의 책임과 시민의 권리를 위한 실질적인 조건이 된다고 할 수 있다.[41] 이러한 이해를 바탕으로 연구자는 시민 상호간, 시민과 국가 공동체간의 이익 충돌을 조정하는 장을 국가가 보장해야 된다고 본다.

2.4.3 균형의 원리의 법적 실현

사적 권리와 공익 간 균형을 달성하는 방법론에는 규범조화와 이익형량이 있다. 우선 이익형량은 충돌법익상호간에 우열을 인정하여 특정한 이익을 우선시키는 방법이다.[42] 추상적으로 충돌하는 법익 상호간에 일정한 위계질서를 인정하여 그 우열을 결정하는 방법이다. 하지만 이러한 형량방법은 기본권과 공익 간이라는 추상적인 가치의 서열을 인정할 수 없다는 점에서 받아들이기 어렵다. 따라서 구체적인 상황을 고려한 이익형량의 방법을 고려해야 한다.

비례의 원칙은 공법과 사법 분야 전반에 걸쳐 적용되는 법의 일반원칙으로서 헌법에서는 기본권을 제한하는 입법에 대한 헌법적 한계를 부여하는 원칙으로 사용되고 있다. 헌법상의 비례의 원칙은 기본권을 제한하는 입법이 추구하려는 “목적과 수단 사이의 관계를 규율하는 원칙”으로서 수단이 항상 목적에 비추어 정당화될 것을 요구한다.

비례의 원칙은 첫째, 권리를 제한하려는 목적이 정당하여야 한다는 것이다.

41) 박정훈, 2005, 행정법의 체계와 방법론, 서울, 박영사: 247-259면.
42) 허영, 2012, 한국 헌법론, 서울, 박영사: 271-275면.

예를 들어, 이차 활용이 정보주체의 동의를 얻지 아니하고 다른 법률에 의해 가능하다고 하더라도 그 목적이 정당해야 한다. 헌법 제37조는 국민의 기본권을 제한하는 헌법적 제한사유를 규정하고 있다. 예를 들면, '국가안보', '질서유지', '공공복리' 라는 목적에 따라 구체적으로 기본권을 제한할 수 있다.

둘째, 제한하는 조치가 목적을 달성하는 데 적합한 수단이어야 한다는 것이다. 예를 들면, 개인정보를 수집하고, 처리하고, 공유하는 등의 조치가 해당 목적을 달성하는데 별다른 효과를 기대하기 어렵다면 그 수단은 적합하다고 할 수 없다.

셋째, 정당한 공적 과제의 이행을 하는 경우라도 적합한 방식으로 필요한 최소한으로 이루어져야 한다는 것이다. 가령 공공기관 간 정보공유를 할 때는 개인 식별자를 익명화하는 것이다.

넷째, 제한이 불가피하고 최소한으로 이루어지는 경우라 하더라도 법익의 균형성이 요청된다는 것이다. 즉 실현하려는 이익과 침해되는 이익을 비교할 때 실현하려는 이익이 월등하게 더 커야 한다.[43]

비례의 원칙은 우위나 서열에 기초한 이익형량의 방법과는 달리 양 법익의 비례적 정서를 목표로 한다. 그래서 비례의 원칙은 충돌하는 법익이 모두 보호할 가치가 있다는 것을 전제하고서 구체적인 상황 속에서의 양 법익간의 관계를 고려할 것을 요구한다.

양창수 교수에 의하면 소유권, 계약, 불법행위 등은 하나의 사회적인 제도로서 다른 모든 개인의 자유나 권리와 조화될 수 있도록 유지·발전되어야 한다고 한다.

---

43) 헌재 1990. 9. 3. 89헌가95; 대판 1994. 3. 8. 92누1728: "국민의 기본권을 제한하는 것으로서 국가안전보장, 질서유지 또는 공공복리를 위하여 필요한 것이 아니거나, 또는 필요한 것이라고 하더라도 국민의 자유와 권리를 덜 제한하는 다른 방법으로 그와 같은 목적을 달성할 수 있다든지, 위와 같은 제한으로 인하여 국민이 입게 되는 불이익이 그와 같은 제한에 의하여 달성할 수 있는 공익보다 클 경우에는 이와 같은 제한은 비록 자유와 권리의 본질적인 내용을 침해하는 것이 아니더라도 헌법에 위반되는 것이다."

그는 “각 개인의 자유로운 자기형성을 공동체보다 앞세우는 이념이 민법에 투사된 것이 바로 사적 자치의 원칙”이라고 한다.[44] 하지만 어떤 권리가 주어졌다고 해서 이를 무차별하게 추구해 나간다면, 법이 궁극적으로 추구하는 평화와 질서는 달성되기 힘들기 때문에 ‘사회적 형평’ 내지는 ‘권리의 사회적 책임성’이라는 이념이 사적 권리행사에 포함되어야 한다고 주장한다. 이런 점에서 비례의 원칙은 사적 권리와 공익 둘 중 어느 하나도 포기하지 않고 양자 간 적절한 균형을 유지해야 한다는 실제적 조화의 원칙과 연결된다.

실제적 조화란 하나의 규범이 다른 규범과 대립되지 않도록 해석하여야 한다는 것을 조건으로 한다. 즉 헌법상 보호되는 법익 간에 충돌이 일어났을 경우, 다른 법익을 희생하여 하나의 법익만을 실현시켜서는 안 되며, 양 법익이 동시에 실현될 수 있도록 해야 한다는 것이다. 여기서 중요한 점은 양 법익이 최적으로(optimal) 실현될 수 있는 경계가 그어져야 하는데, 그 경계획정(境界劃定)은 그때그때의 구체적 사례에 있어서 비례적이어야만 한다.

이러한 맥락에서 상호이해와 합의가 정보주체의 자기결정권 행사와 공익을 위한 이차 활용의 긴장 관계를 풀 수 있는 내적 구조라고 할 수 있다. 이때 국가의 역할은 정보화 시대를 사는 개인과 공동체, 이들의 사회적 요구와 공동의 가치[45]를 최대한 실현시킬 수 있도록 돕는 것이다. 공익을 위한 사적 권리의 제한이라는 이념과 민감정보이기 때문에 각별히 취급해야 하며 오히려 국가가 나서서 이를 보호해야 한다는 이념을 조화시키는 노력이 필요하다.

이어지는 장들에서는 이러한 조화를 이끌어 내도록 지지해 주는 법적 근거들을 검토하고와 그 타당성을 고찰해 본다. 그리고 개인정보를 다루는 사람들이 법적

---

44) 양창수, 2000, 민법입문(신수판), 서울, 박영사: 354면 이하 참조.

45) Michael J. Sandel, 1982, Liberalism and the Limits of Justice, Cambridge, Cambridge University Press: pp. 170-179.

요건을 충족하기 위하여 공통적으로 수행하는 절차를 검토함에 있어서도 사적 권리와 공익간의 균형 관점에서 접근하고자 한다. 이러한 균형을 이차 활용의 기본적인 틀로서 상정하고, 민감정보가 수집·저장·관리·제공되는 정보처리의 과정과 프라이버시 보호 개념을 적용한 시스템설계를 포함한 논의를 전개하고자 한다.

제3장 공공정보의 이차 활용과 개인정보의 보호

프라이버시가 언급될 때는 불가피하게 인간의 삶을 공적 영역과 사적 영역으로 구분하게 된다. 이러한 구분은 자신의 정체성이 식별 정보로서 표현되는 정보화 사회에서 더 필요해진다. 하지만 공공기관이 수집·보유·관리하는 개인정보는 공적 영역에 맡겨졌기 때문에 정보주체의 권리까지도 공공기관에 있다고 간주해야 하는지는 더 따져볼 필요가 있다.

공공정보에 포함된 개인정보는 공적 영역에서도 여전히 개인의 정체성을 표현하기 때문에 그의 이용을 위해서는 정보주체의 사적인 프라이버시 보호가 필요해 보인다. 일종의 공공재로서 공공정보를 활용할 수 있다는 입장에서는 이차 활용이 가져다주는 효용과 효율을 앞세우겠지만, 프라이버시침해의 우려를 수인할 만큼의 유용성이 있는지, 이차 활용에 있어 다른 문제점은 없는지 검토할 필요가 있다.

자기의 개인정보에 대한 통제를 의미하는 개인정보자기결정권은 개인정보의 오·남용을 막기 위한 안전장치로서 정보주체에게 개인정보의 수집·이용·가공·제공 처리 과정에 일정하게 참여할 수 있는 기회에 대한 권리이다. 정보주체가 정보처리에 참여하는 방법은 동의를 통해서인데, 동의가 있으면 원칙적으로 제한 없이 개인정보의 수집·이용·활용이 허용된다. 그리고 다른 법률에 별도의 규정이 있으면 동의가 없이도 이차 활용할 수 있다. 공공기관은 다른 법률이 적용되는 기관이며, 따라서 공공기관이 보유·관리하는 공공정보도 별도의 법규정에 의하여 정보주체의 동의 없이 활용될 수 있다.

제3장에서는 공공정보의 이차 활용을 가능하게 한 정보화의 특징과 정보화에 따른 문제점에 대하여 검토하고, 현행법상 공공정보의 이차 활용을 가능케 하는 법 규정을 살펴본 후, 현행법제의 한계를 지적하고자 한다.

3.1 정보화와 공공정보의 이차 활용

행정서비스의 보다 효율적인 성과를 이끌어 내는데 공공정보를 활용하고자 하는 '정부 3.0'의 패러다임은 우리나라의 높은 전자정부의 수준에서 기인한다고 생각된다. 중앙정부의 공공서비스 제공을 위한 정보통신서비스의 수준을 측정하는 종합적 지표인 UN 전자정부발달지수(e-Government Development Index)[46]에서 우리나라는 193개국 중에서 2010년에 이어 2012년에도 1위(World e-government development ranking)에 랭크되어 있다(표 2).

표 2. 세계 전자정부 발달지수

Country	E-government development Index	
	2012	2010
Republic of Korea	0.9283	0.8785
Netherlands	0.9125	0.8097
United Kingdom	0.8960	0.8147
Denmark	0.8889	0.7872
United States	0.8687	0.8510
France	0.8635	0.7510
Sweden	0.8599	0.7474
Norway	0.8593	0.8020
Finland	0.8505	0.6967
Singapore	0.8474	0.7476

정보통신기술을 정부의 서비스와 행정업무 수행에 활용하게 되면서 개인정보는 오히려 자발적인 제공에 의하여 수집되고 그 활용도 다양하게 더 많이 이루어지고 있다.

46)UN, E-Government Surveys, 2010 : p. 60; UN, E-Government Surveys, 2012: p. 25.

공공정보는 구조적인 데이터[47]가 대부분을 차지한다. 주로 행정서비스의 수행 과정에서 생성되거나 취득되므로 대부분 일정한 규칙에 따라 수집되고, 정해진 서식에 따라 관리되는 정보들이기 때문이다. 그리고 공개와 공유를 위한 플랫폼으로서 웹(World Wide Web)을 사용하고 매시업(Mashup)[48]등을 적용하며 비독점적인 포맷이 채택된다. 이러한 특징들은 여러 자료원으로부터 제공받은 정보를 다양한 목적으로 분석하는 이차 활용이 더 용이하게 이루어질 수 있도록 한다. 그림 3은 공공기관이 개인정보를 수집하여 수집목적 내에서 처리하는 단계와 이차 활용을 위해 다시 개인정보를 처리하는 단계를 도식화한 것이다.

그림 3. 개인정보의 이차 활용단계 및 조건

47) 데이터의 어떠한 요소아래 어떤 요소가 있고, 그 아래 다른 요소가 있는 구조를 가진 것을 말한다. 데이터베이스 내부의 데이터에 유기체적 성질을 부여하여 원하는 목적으로 분석되도록 하기 위하여 웹상에 존재하는 개별 데이터요소를 식별하고, 그 정보를 부여하고 상호 연결이 용이한 데이터이다. 위키 백과.
http://ko.wikipedia.org/w/index.php?search=%EA%B5%AC%EC%A1%B0%EC%A0%81+%EB%8D%B0%EC%9D%B4%ED%84%B0&title=%ED%8A%B9%EC%88%98%3A%EA%B2%80%EC%83%89&go=%EB%B3%B4%EA%B8%B0

48) 웹으로 제공하고 있는 정보와 서비스를 융합하여 새로운 소프트웨어나 서비스, 데이터베이스 등을 만드는 것을 말한다. 인터넷에서 제공하는 다양한 오픈 API를 활용하여, 새로운 아이디어와 서비스를 개발하는 것을 말한다. 위키 백과.
http://ko.wikipedia.org/wiki/%EB%A7%A4%EC%8B%9C%EC%97%85_(%EC%9B%B9_%EA%B0%9C%EB%B0%9C)

공공기관은 수집된 개인정보를 애초의 목적 범위 내에서 최소한으로 이용한다. 이차 활용은 이 단계를 벗어나 목적 외의 용도로 활용하는 것이다. 만약 외부로 제공하거나 공개·개방하기 위해서는 다른 법률에 근거가 있거나 정보주체에게 동의를 받거나 비식별화 조치를 해야 한다.

정보주체는 공공기관이 공공서비스를 제공하기 위하여 수집·관리·보유하는 정보에 대해서는 염려하지 않는다. 앞서 언급한 사적 권리의 침해라고 생각하지 않는다. 즉 원치 않은 사람에게 사생활이 노출된다고 생각하지 않으므로 자기정보결정권이 침해된다고 여기지 않는다. 이러한 믿음의 저변에는 정부 내지는 공공기관에 대한 무비판적인 신뢰가 있기도 하고, 개인정보보호법이라는 법적인 안전망에 대한 신뢰가 있기도 하다. 그러나 간과해서는 안 되는 점은 공공기관의 정책결정에 대한 재량권이 확대되면 불가피하게 나름대로의 가치 판단이 개입한다는 사실이다.

따라서 이차 활용을 해야 하는 정당성을 공익에서 찾을 경우, 이러한 가치 판단의 문제는 더욱 중요시되고,[49] 결국 정보주체의 자기결정권의 행사와 공익의 균형을 어디서 찾을 수 있는지가 쟁점으로 드러나게 된다.[50] 이점은 개별적인 다양성을 수용한 정책을 수립의 중요성을 일깨운다. 즉 하나의 우월한 가치에 따르는 것에서 벗어나서 개개인에게 부여된 권한을 중요시여기고, 절차를 통해서 그 목소리를 받아들이는 제도가 필요함을 시사한다.

과학기술의 가치는 활용하는 사람의 의도와 목적에 따라 달라진다. 말하자면, 기술 자체가 가지고 있는 속성 때문에 특수하게 문제가 발생하지는 않는다. 공공정보의 이차 활용에 대한 문제는 누가 어떤 목적을 위해 정보처리를 할지 모른다는 불확실성과 그로 인한 두려움으로 인해 발생한다고 볼 수 있다. 이러한

49) Richard E. Flathman, 1966, The public interest: An essay concerning the normative discourse of politics. New Jersey, Wiley: pp. 1-2.

50) Dwight Waldo, 2006, The administrative state: A study of the political theory of American public administration. New Jersey, Transaction Publishers: pp. 13-89, 100-129.

불확실성과 두려움이 국가와 개인의 공동의 문제라고 여기는 것에서부터 공공정보의 정보주체에 대한 권리를 어떻게 보호할 수 있는지에 대한 논의를 시작할 수 있을 것이다.

3.2 공공정보 이차 활용의 법적 근거

국내에서 공공정보 활용에 대한 관심은 1998년 '공공기관의 정보공개에 관한 법률'이 시행되면서 점차 커지게 되었다. 동 법률에 따르면, "공공정보"란 공공기관이 직무상 작성 또는 취득하여 관리하고 있는 문서(전자문서를 포함한다. 이하 같다)·도면·사진·필름·테이프·슬라이드 및 그 밖에 이에 준하는 매체 등에 기록된 사항을 말한다.[51]

한편, 2013년 제정·시행된 '공공데이터의 제공 및 이용활성화에 관한 법률'에서 정의하는 "공공데이터"란 데이터베이스, 전자화된 파일 등 공공기관이 법령 등에서 정하는 목적을 위하여 생성 또는 취득하여 관리하고 있는 광(光) 또는 전자적 방식으로 처리된 자료 또는 정보를 말한다.[52] 본 논문에서는 공공기관이 생성·취득·관리하고 있는 전자화된 정보를 공공정보라고 정의한다.

우리나라에서 공공기관이 보유하고 있는 정보를 효율적으로 관리할 뿐만 아니라 공공기관 간 공동 활용의 의지를 천명한 것은 1998년 3월 28일에 제정되었다가 2001년 6월 30일 폐지된 '행정정보공동이용에 관한 규정'에서 그 시원을 찾을 수 있다. 공공정보의 공동 활용은 곧 이차 활용을 가능하게 한 조치인 동시에 법적 근거가 되었다. 현행법상 이차 활용을 위한 법적 근거는 '통계법',[53] '공공데이터의 제공 및 이용활성화에 관한 법률',[54] '전자정부법',[55] '공공기관의 정보공개에 관한

51) 공공기관의 정보공개에 관한 법률 제2조.
52) 공공데이터의 제공 및 이용 활성화에 관한 법률 제2조.
53) 1962.1.15 제정, 법률 제 980호, 2014.5.14., 일부개정, 법률 제 12571호.

법률'[56]에서 찾을 수 있다.

'통계법'은 행정기관의 자료 및 전산망을 이용할 수 있는 법적 근거이다. 하지만 사법기관의 자료를 이용할 수 있는 근거는 없었기 때문에 혼인·출생·사망 통계 작성에 활용하기 위하여 공공기관의 범위에 사법기관 등을 포함하고 국가 통계 작성에 효율성을 높이려는 목적으로 개정되었다.

'공공기관의 정보공개에 관한 법률'은 공공기관의 정의를 명확히 하고 있으며, 국민의 알권리 확대 및 행정의 투명성 제고를 위하여 사전에 공공정보를 공개하기 위한 목적에서 제정되었다. 따라서 공개하기로 분류되는 정보가 어떤 것인지가 핵심이며, 이를 결정하는 주체인 정보공개심의위원회의 역할이 중요하다.

'전자정부법'은 국민중심의 수요자 맞춤형 행정서비스를 제공하기 위하여 제정되었다. 즉 건강검진, 제세·공과금 납부 등에 관한 생활정보를 통합전자민원창구를 통하여 열람할 수 있도록 하고 있다. 그리고 중앙행정기관의 장 등이 국민에게 제공하는 재화, 서비스 등 공공서비스의 목록을 제공하도록 하고 있다. 또한 행정기관 등이 데이터를 공동으로 활용할 수 있도록 행정자치부장관이 데이터 활용 공통기반시스템을 구축할 수 있도록 하였다.

'공공데이터의 제공 및 이용활성화에 관한 법률'은 스마트 폰 대중화에 따라 교통, 기상, 공간, 복지, 보건, 식품, 관광, 환경 등 국민의 생활전반에 걸쳐 생성된 공공데이터를 국민이 최우선적으로 이용할 수 있도록 보장하려는 목적으로 제정되었다. 이 법에 따라서 공공기관은 공공데이터 제공의무를 부담하게 되었다. 동 법률을 근거로 공공데이터는 그 기준에 따라 민간에게도 제공될 수 있으며, 개별 공공기관에 산재되어 있는 공공데이터의 효율적인 제공과 이용을 지원하기 위하여 공공데이터활용 지원센터를 설치·운영하고 있다.[57]

---

54) 2013.7.30 제정, 법률 제11956호, 시행 2013.10.31.

55) 2001.3.28 제정, 법률 제6439호, 2014.1.28., 일부개정, 법률 제12346호.

56) 1996.12.31 제정, 법률 제5242호, 2013.8.6., 일부개정, 법률 제11991호.

57) 국가정보화 기본법 제14조.

3.3 공공정보의 이차 활용과 관련한 문제점

공공정보의 이차 활용은 보다 다양한 분야에서 더욱 편리한 공공서비스를 도모하기 위한 정보화 시대의 효율적인 방법론이자 피할 수 없는 시대적 요청이다. 하지만 동시에 수집된 개인정보의 목적 외 이용, 공공기관간의 공유 또는 링크를 통하여 정보주체가 인지하지 못한 채 내 정보가 노출될 수도 있다는 점에서 개인정보자기결정권이 침해되는 측면도 있다.

개인정보에 관하여 정보주체가 행사하는 사적 권리는 개인정보자기결정권이며, 만일 이 권리를 제한할 경우가 있다면, 그 이유는 정당한 공익의 목적 때문이다. 공익 목적이라면, 원래의 수집목적 이외의 다양한 분야에서 공동 이용할 뿐만 아니라 공공기관 간에는 정보주체의 동의를 획득하지 않고도 이차 활용할 수 있다. 비록 개인으로부터 수집된 정보라도 공공정보이기 때문에 동의가 면제된 채 활용할 수 있는 것이다. 그러나 비록 공공기관이 보유·관리하고 있어 그 성격이 공공정보라 할지라도 민감정보는 정보주체가 다른 사람에게 위임하거나 양보할 수 없는 프라이버시 핵심영역에 있다.

공익이라는 목적 달성과 프라이버시 보호라는 두 이익간의 우열을 가릴 때, 양보할 수 없는 가치를 갖는 양자 모두 그 작용을 발현하고, 하나의 법익이 다른 법익 때문에 절대적으로 차단되지 않도록 하는 일은 중요하다. 그런데 공공정보를 이차 활용할 때는 다른 법률에 근거하여 개인정보자기결정권을 행사할 수 없는 경우가 발생한다. 말하자면, 공익을 위해 이차 활용되는 경우, 동의가 면제되며 이는 사적 권리의 제한이 된다.

공익이라는 목적이 전제된다면, 이차 활용을 할 수 있고, 이때 익명성을 전제로 동의가 면제된다. 익명성이 보장된다는 전제하에 동의를 면제하지만, 이차 활용은 재식별의 위험이 매우 높다는 것이 다시 문제가 된다. 그렇다면 이차 활용의

공익에 비추어 사적 권리의 포기를 이익형량을 근거로 의제하는 것 자체가 무리가 있다. 또한 이차 활용을 심의·의결하는 위원회에서 일반적인 개인정보와 똑같은 절차로 민감한 개인정보에 대해서도 이익형량을 한다면, 정보주체 모두가 수인하기에는 부족한 법적인 흠결이 있어 보인다.

이차활용과 관련된 공공정보 요청-제공 체계의 문제점을 그림 4와 도식화 하였다.

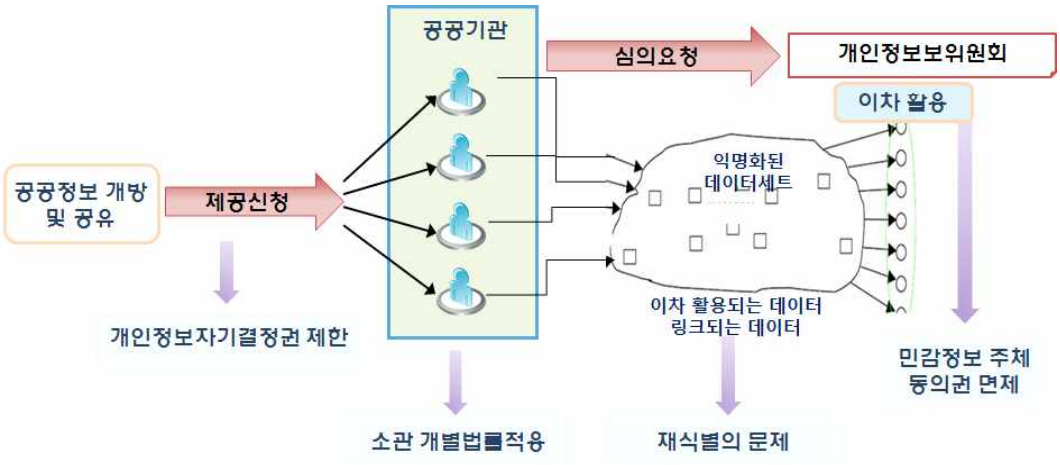

그림 4. 이차활용을 위한 공공정보 요청-제공 체계의 문제점

요약하면, 우선 공공정보를 이차 활용하기 위해서는 '공공데이터의 제공 및 이용활성화에 관한 법률'에 근거하여 공공기관에 공공정보제공을 신청할 수 있다. 이때 정보주체의 동의는 면제되고, 공공기관은 개별 소관 법률에 근거하여 제공할 수 있다. 그리고 그 적법성의 심의를 위하여 개인정보보호위원회에 심의·의결을 요청할 수 있다. 하지만 민감정보의 이차 사용에 관하여는 정보주체의 사적 권리 보호와 공익간의 이익형량에 있어서 그 균형점을 찾는 것 같아 보이지 않는다.[58]

이차 활용되는 정보는 비록 익명화를 하였다 해도 재식별의 위험이 있다. 재식별된 정보에 관한 정보처리를 위한 법적·기술적 절차는 아직 마련되어 있지 않다. 이와 같은 문제점을 국내법의 법률체계 속에서 구체적으로 하나씩 살펴보도록 한다.

3.3.1 정보프라이버시에 대한 개인 간 인식의 차이

개인정보보호에 관한 이슈의 등장은 프라이버시에 기초하고 있다. 하지만 프라이버시라는 개념과 프라이버시권이라는 권리개념에는 차이가 있다.[59] 법이 평가하는 것은 무엇이 프라이버시인가가 아니고, 어떠한 환경에서 프라이버시가 법적 보호의 영역[60]에 속하는가이다. 즉 프라이버시에 대한 법적 보호정도를 어디까지 확대 할 수 있느냐 하는 범위의 문제가 쟁점이다.

세계 최초로 프라이버시 보호 영역에 대한 법적 관여가 이루어진 것은 1878년에 미국의 쿨리(Thomas Cooley) 판사가 민사상의 손해배상(Tort)에 관한 저서에서 프라이버시권이라는 법적 개념을 제시하면서부터다.[61] 이 저서에서 프라이버시권은

---

58) 제 11회 개인정보보호위원회의, 2013. 6. 24., 연구대상 환자의 건강정보 및 의무기록 제공 요청에 대한 심의·의결 요청 건; “사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보 등 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보인 민감정보는 유출시 사회적 차별을 야기하거나 인권을 현저히 침해할 우려가 있어 동 정보의 처리는「개인정보보호법」제23조에서 별도로 규율되고 있다. 따라서 한국보건의료연구원이 의료기관들로부터 민감정보와 주민등록번호는 함께 제공받아야 의미가 있으며, 민감정보의 처리 가능여부는「개인정보보호법」제18조 제2항 제5호에 의한 판단이 아니라 동 법제23조 제2호에 의한 판단에 따라야 할 사안이므로 한국보건의료연구원의 신청을 각하한다.”

59) 권헌영, 2004, “전자정부환경에서의 개인정보보호법제에 관한 연구”, 연세대학교 대학원, 박사학위논문: 32면.

60) Hyman Gross, 1967, "The Concept of Privacy", 42 N.Y.U.L. Rev. 34: p. 36; “To make good the claim that privacy is indeed noticed and protected, preliminary indication of the range of legal protection is in order."

61) Thomas McIntyre Cooley, 1878, A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract, 1st ed., Chicago, Callaghan and Company: p. 29

‘홀로 있을 권리(the right to be let alone)’를 뜻했다.[62] 1890년에 이를 보다 상세하게 분석한 논문에서 웨렌과 브렌다이스(Warren, S. D., & Brandeis, L. D.)는 ‘프라이버시권은 진보된 문명세계에서 살고 있는 개인에게 필수적인 것’ 이라고 주장했다.[63] 이러한 주장들은 당시의 황색신문들이 유명인의 사생활을 들추어내어 그것을 상업적으로 악용하는 사례가 많아지면서 이에 대한 법적 대응의 한 형식으로 대두된 것이다.

그 후 1965년 미 연방대법원의 판결[64]은 프라이버시권을 통하여 보호되는 법익은 두 가지 측면이 있다는 사실을 밝혀주었다. 즉 ‘사적인 사항이 공개되지 않음으로써 얻을 수 있는 이익’과 ‘자신에 대한 중요한 문제를 자율적이고 독자적으로 결정함으로써 얻을 수 있는 이익’이다. 프라이버시권에 대한 개념규정의 시도는 그 후에도 많은 학자들에 의해 있었으나 충분한 성공을 거두지 못하는 것으로 보인다.[65]

1980년대 이후 컴퓨터의 발달에 따라 개인정보를 전자적 형태로 무한히 축적할 수 있게 되자 타인의 수중에 있는 개인정보에 대한 정보주체의 통제권을 나타내기 위해 ‘정보프라이버시(information or informational privacy)’라는 개념을 사용하기 시작하였다.[66] 특히 제리 강(Jerry Kang)은 정보프라이버시를 개인정보를 취득, 공개, 이용하는 조건을 통제할 수 있는 개인의 청구권으로 정의하였다.[67] 그에 의하면

---

62) Louis Dembitz Brandeis, 1928, *case of Olmstead v. United States*, “the right to be let alone. the most comprehensive of rights and the right most valued by civilized men.” Although the Constitution does not mention a right to privacy, the Supreme Court has inferred it from the language of the First, Third, Fourth, Fifth, and Ninth Amendments.

63) Samuel D. Warren & Louis D. Brandeis, 1890, “The Right to Privacy”, 4 Harv. L. Rev: pp. 193-195.

64) Griswold v. Connecticut, 1965, 381 U. S. 479.

65) Colin J Bennett, 1992, Regulating Privacy: Data Protection and Public Policy in Europe and the United States, Ithaca, NY, Cornell University Press: p. 25.

66) Joel L. Rosenbaum, 1998, “Privacy on the Internet: Whose Information Is It Anyway?”. Jurimetrics Vol. 38 No. 4: pp. 565-573.

67) *Ibid.,* pp. 1202-1203.

개인정보(personal information)는 개인을 식별할 수 있는 정보(information identifiable to the individual)이다. 즉 사소한 것이든 민감한 것이든 개인을 식별할 수 있는 것으로서 그 개인에 대한 귀속관계(authorship relation to the individual), 그 개인에 대한 묘사관계(descriptive relation to the individual), 그 개인에 대한 기계적 도식관계(instrumental mapping relation to the individual) 모두를 포함한다.

'귀속관계'는 전화통화, 이메일과 같은 것이고, '묘사관계'는 성별, 신장, 지문, DNA, 혹은 건강상태 등과 같은 개인의 생체상태로 서술할 수 있고, 성적 취향, 범죄기록과 같이 개인의 역사적 사실과도 관계 지을 수 있다. 또 종교, 정당 가입여부와 같이 사회적 관계를 설명해주기도 한다. '기계적 도식관계'는 주민번호를 예로 들 수 있겠다. 이들 세 가지 범주는 상호 배타적이지 않고, 어떤 정보가 '개인적'일 수 있는지 가늠할 수 있는 개념을 제공한다.[68]

제리 강의 입장은 개인정보를 개인의 자율성, 인격성의 관점에서 바라보는 것으로서 개인정보보호의 문제를 은닉 상태의 유지여부보다는 자신에 관한 정보의 자율적 통제에 더 초점을 맞춘 것이라고 할 수 있다. 무엇보다 정보프라이버시권이 사회와 격리된 채 주장할 수 있는 사생활영역의 권리가 아니고, 오히려 사회에 참여하는데 필요한 사회적 영역의 권리라는 점이다. 그래서 인간으로서의 존엄과 가치를 실현하고 행복을 추구하기 위하여 '개인이 자신에 관한 정보가 어디까지 이용되는가를 자유롭게 통제할 수 있는 것이 자기결정권'이다. 이 권리는 정보사회에서 기본권으로서 정보프라이버시권[69]이라고 정의할 수 있다.

우리나라 개인정보보호법 제23조는 개인정보보호의 자율성에 대한 문제를 규정하고 있다. 동 법은 민감정보의 유출이 정보주체의 사생활을 현저히 침해할

---

68) Jerry Kang, 1998, "Information Privacy in Cyberspace Transactions". Stanford Law Review no. 50: pp. 1202-1203.

69) *Ibid,* pp. 1193 - 1294; Information Privacy in terms of shielding one's own physical space(spatial privacy); preserving one's own ability to make choices(decisional privacy); and controlling the processing of information about oneself(informational privacy).

우려가 있기 때문에 묘사관계의 개인정보유출을 금하고 있다.[70] 이는 정보주체의 사생활의 불가침을 보장받을 수 있는 권리,[71] 개인의 양심 영역이나 성적 영역과 같은 내밀한 영역에 대한 보호, 인격적인 감정세계를 존중하는 권리와 정신적인 내면생활이 침해받지 아니할 권리로서 정보프라이버시권을 보호하기 위한 규정이라고 할 수 있다.[72]

그러나 정보프라이버시에 근거한 개인정보보호 관련법들은 오히려 새로운 정보통신기술의 발달로 인해 프라이버시 침해의 증가는 당연하다는 것을 밝혀줄 뿐 침해를 방지하거나 정보주체에 대한 충분한 구제조치를 마련해주지 못하고 있다는 비판이 있다.[73] 이런 비판은 개인정보의 이용과 보호의 문제에 있어 관점이나 인식의 차이로 인해 발생한다고 볼 수 있다. 예컨대, 어떤 개인은 정부가 자신의 정보를 디지털로 수집하고 관리하는 것 자체에 민감한 반응을 보이는가 하면, 또 다른 개인은 수집된 정보로 인해 정부로부터 보호를 받는다고 느끼기도 한다. 따라서 개인정보의 수집·활용에 대하여 전적으로 개인의 자유 또는 자기결정권의 침해라는 입장은 문제일 수 있다.

개인은 공공기관이 보유·처리하고 있는 자신의 정보를 그 효용성과 위험성의 평가에 따라 보호수준을 강하게 설정할 수도 있고, 이용의 가치를 우선하여

---

70) 개인정보보호법 제23조: 개인정보처리자는 사상·신념, 노동조합정당의 가입·탈퇴 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보를 처리하여서는 아니 된다.

71) 헌재 2007.5.31. 선고 2005 헌마 1139.: 헌법 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.”고 규정하고 있는바, 여기서 말하는 사생활의 비밀은 국가가 사생활 영역을 들여다보는 것에 대한 보호를, 사생활의 자유는 국가가 사생활의 자유로운 형성을 방해하거나 금지하는 것에 대한 보호를 의미한다. 구체적으로는 개인의 내밀한 내용의 비밀을 유지할 권리, 개인이 자신의사생활의 불가침을 보장받을 수 있는 권리, 개인의 양심영역이나 성적영역과 같은 내밀한 영역에 대한 보호, 인격적인 감정세계의 존중의 권리와 정신적인 내면생활이 침해받지 아니할 권리 등으로 설명된다.

72) 헌법 제17조: 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.

73) Colin J. Bennett and Charles D. Raab, 2006, The Governance of Privacy-Policy Instrument in Global Perspective, Cambridge MA, MIT Press: p. 147.

보호의 수준을 낮게 설정할 수도 있다. 즉 정보주체가 그 위험성을 자신이 정보의 객체로 전락하여 타인에게 노출된 대상일 뿐이라고 느낀다면 불안감 때문에 위험성을 높게 책정하여 강한 보호를 요구할 것이다. 이렇게 개인 간 인식차가 보호와 활용간의 균형을 찾는 작업, 더 나아가 합의에 기초한 법제개선을 모색하는데 있어서 장애가 될 수도 있다.[74]

3.3.2 동의 방식·범위의 문제점

우리나라 개인정보보호법은 개인정보의 처리에 있어서 그 목적이 수집단계에 미리 명확히 특정되어 있어야 할 뿐만 아니라 그 이후의 처리단계에 있어서도 수집시의 특정된 목적과 일치되게 저장 또는 이용되어야 한다는 목적구속의 원칙[75]을 적용하고 있다. 목적구속의 원칙은 한편으로는 개인정보의 처리목표를 확정하고 다른 한편으로는 그 처리범위를 한정하는 역할을 한다. 즉, 정보주체의 기본권 제한이 그것을 통해 추구되는 목적과 비례관계에 있도록 그 정보를 활용하는 목적이 정당해야 하며, 목적을 달성하는 방법도 적합한 수단이어야 한다는 의미이다.

현행법률 체계는 공공정보의 이차 활용을 위하여 예외를 적용하려면 법률에 정해진 그 별도의 목적에 따라야 한다. 즉 동일한 개인정보를 이차 활용하지만

---

74) 박정자, 2008, 시선은 권력이다, 서울, 기파랑: 100-152면 참조; 정보주체의 불안감과 안정감은 제레미 밴덤(Jeremy Bentham)의 책 '판옵티콘(Panopticon)'에 잘 설명되어 있다. 즉 감시자에게는 통제 가능한 다수 중의 하나이며, 갇힌 사람에게는 자신이 항상 누군가에게 보이고 있다는 의식을 심어 주는 판옵틱의 주요 효과를 설명한다. 판옵틱의 효과는 개인정보를 통하여 누군가 자신을 지배할까봐 불안해하고 프라이버시가 침해되었다고 인식하게 된다는 것이다.

75) 이 원칙에 관한 입법례로는 OECD의 '프라이버시 보호와 개인데이터의 국제적 유통에 관한 가이드라인' 제9조, UN의 '전산화된 개인정보 파일의 규율에 관한 가이드라인' 제3원칙, EU 1995 '개인데이터의 처리와 개인데이터의 자유로운 유통에 관련된 개인정보 지침' 제 6조, 영국 데이터보호법 제 2원칙 등이 있다.

그 목적별로 다른 규제를 할 수 있다. 예를 들어 이차활용이 많은 의생명과학 연구를 위한 법적 근거인 '생명윤리 및 안전에 관한 법률'상 개인정보 개념은 개인정보보호법상의 개인정보 개념[76]보다 더 넓게 규정되어 있다. 동 법률에서는 "개인정보"란 개인식별정보(배아·난자·정자 또는 인체유래물 기증자의 성명·주민등록번호 등 개인을 식별할 수 있는 정보), 유전정보 또는 건강에 관한 정보 등 개인에 관한 정보를 말한다.

문제는 공적인 목적을 위한 이차 활용을 위하여 결정을 내릴 때 정보주체에게 직접 수집한 것이 아니기 때문에 어떤 법률의 개념을 적용할 것인지 혼란의 소지가 있다. 또한 정보주체에게 동의를 얻지 않는 것도 다른 법률에 의해 정당하게 활용될 수 있는데, 소관 분야에 제정된 개별 법률에 따라 관련된 행정기관의 장이 지도·감독권을 행사하므로 그 목적에 대한 정당성 확보에 어려움이 있을 수 있다.

이와 같은 문제점을 구체적인 상황에서 살펴보면, 공공정보의 이차 활용은 대부분 최초 수집된 공공기관이 아닌 제3자에게 이전된 정보를 활용하게 된다. 그리고 한 기관의 공공정보가 아니라 여러 기관에 요청하여 재 수집된 정보를 함께 이용하는 것이 보통이다.[77] 이러한 경우에는 정보처리과정에 정보주체의 의사가 반영될 기회가 희박하다. 왜냐하면 공공기관의 제3자 제공은 제한 없이 허용되기 때문이다. 개인정보의 제3자 제공의 허용요건은 개인정보보호법에 명시되어 있다. 일반개인정보를 제3자에게 제공할 수 있는 '일반적 허용기준'을 제17조 제1항에서 정하고, 제18조 제2항에서는 '예외적 허용기준'을 정하고 있다.[78]

---

76) 개인정보보호법 제2조: 개인정보는 "살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

77) 개인정보보호법 제2조, 제3조, 제 6조.

78) 개인정보보호법 제18조 2항; "통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서

또한 각 개별분야에 대해 별개의 특별 법률로 예외규정을 우선 적용하여 이차 활용 및 활용 활성화에 대한 근거를 제시하고 있다. 예외적 허용기준에 의하여 이차 활용의 적법성과 정당성을 찾을 수 있으나 수집당시의 '동의'[79] 효력이 여전히 존재하는지는 따져 봐야 할 문제이다. 같은 맥락에서 생명윤리 및 안전에 관한 법률'에서 인간 대상 연구의 연구 대상자에게 요구하는 '서면동의'[80]에서도 비록 정당한 공적 과제를 이행하는 경우라도, 미래의 연구목적이라면 무엇을 정당화해야 할지 모르는 상태이므로 충분한 설명에 의한 동의라고 간주하기는 어렵다.

그러므로 정부나 공공기관이 정보주체의 존엄성과 자율성을 지켜주고 있다는 것을 시민들에게 알릴 기회가 필요하고, 정보주체에게도 자신의 정보가 위법한 공개에 대해서 알고 대처 할 수 있는 기회가 필요하다.[81] 그래야만 공익을 위하여 정보주체의 동의가 면제되는 경우에 그것은 정당한 제약으로서 정보주체의 동의를 얻지 아니하거나 동의의 범위 이상의 것을 할 수 있다. 그리고 개개인도 공익을 위하여 자신의 개인정보자기결정권의 제한을 수인(容認)할 수 있다. 따라서 이차 활용까지 개인정보자기결정권을 관철하려면, 개인정보의 수집·처리·활용에 대한 동의 방식과 범위를 변경할 필요가 있다.

특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우" 예외로 인정한다; 제15조 2항; "1. 개인정보의 수집, 이용 목적, 2. 수집하려는 개인정보의 항목, 3. 개인정보의 보유 및 이용 기간" 등을 반드시 통보하여야 한다.

79) 개인정보보호법 제17조 제3항; 개인정보처리자가 개인정보를 해외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 해외 이전에 관한 계약을 체결하여서는 아니 된다; 제 22조 1항; 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

80) 생명윤리 및 안전에 관한 법률 제37조 제1항 참조.

81) Francis S. Chlapowski, 1991, "The Constitutional Protection of Informational Privacy", Boston University Law Review 133: pp. 133-134.

3.3.3 재식별화의 문제점

정보사회에서 익명성의 불가침은 타인에 대한 예의이자 신뢰관계를 지속할 수 있는 사회적인 약속일 수 있다. 익명성의 요청은 타인의 관심과 식별로부터 벗어나고 싶은 것이며, 사적 영역이 침해받고 싶지 않은 것이다. 타인에 의한 무분별한 관심이나 왜곡된 평가가 자신의 고유한 정체성을 결정한다면 불쾌감을 넘어서 인간으로서의 존엄과 가치마저도 위협받을 수 있다.

익명성의 원칙은 정보주체의 동의는 없으나 정보 활용이 필요하다고 인정되는 경우에 반영하게 된다. 즉 개인정보처리에 있어 정보주체의 식별을 최소화하여 적정한 수준의 익명성이 보장된다면, 정보주체는 자기결정권의 행사를 양보할 수 있다는 것이다.

중요한 것은 익명성 요청이 개인 식별이 가능한 정보뿐만 아니라 그 자체만으로 다른 것과 결합하여 개인을 식별할 수 있는 모든 정보에 적용된다는 것이다. 즉, '개인정보보호법'이나 '정보통신망법'에서 정의하는 '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보'도 익명화의 대상이다. 그렇다면, 개인정보의 핵심은 '개인의 식별가능성'이며, 식별가능성을 최대한 막는 것이 법에서 추구하는 익명화의 의의라고 할 수 있다. 이런 측면에서 본다면, 현행 개인정보보호법에서 익명성을 확보하기 위해 제시하는 방법을 면밀히 재고해 볼 필요가 있다. 그리고 재식별되는 경우도 고려대상이다. 무엇보다 이차 활용과 관련되어 새롭게 제기되는 문제점이 개인정보 비식별화 조치를 한 경우조차도 연결(linkage)[82]을 통하여 '식별가능성'이 있는 정

82) 안전행정부, 전자정부법의 이해와 해설, 2001, 안전행정부: 56면; 우리나라의 공공기관에서 적용하는 행정정보공동이용방식은 다음 네 가지 방식이다. (1) Data integration; 관련 DB의 요약본을 수집하여 하나의 DB로 통합 구축하고 개별수요자에게 제공하는 방식. 이중적 DB가 구축된다는 문제점이 있음. (2) Data pool; 관련 DB의 요약 DB를 수집하여 pool로 관리하고, 통합 활용 시스템에 요약 DB를 제공하는 방식. (3) Data profiling; 일관된 정보를 집

보로 환원될 수 있다는 점이다.

개인정보보호법 및 시행령에 명시된 조항에 따라 고유 식별정보의 안정성을 확보하기 위하여 선택할 수 있는 기술적 보호대책은 표 3과 같은 방법이 있을 수 있다. 개인정보보호법의 조항은 저장·관리단계에서는 구체적인 기술수단을 명시하지 않고 있는 것을 볼 수 있다.

표 3. 개인정보보호법과 선택 가능한 기술적 개인정보보호조치

개인정보보호법 및 시행령	선택 가능한 기술적 보호조치
법 제21조: 개인정보의 파기	영구삭제(S/W, H/W파쇄기)
법 제24조3항: 고유 식별 안정성 확보조치	암호화(DRM/DB, file암호화)
법 제 33조: 개인정보 영향평가	개인정보식별시스템 개인정보유출차단시스템(DLP)
령 30조1항2: 개인정보에 대한 접근통제 및 권한의 제한조치	접근권한관리
령 30조1항3: 개인정보가 안전하게 저장·전송 될 수 있도록 하기위한 암호화 등 조치	개인정보 전송관리시스템
령 30조1항4: 접속기록의 보관 및 위조·변조방지를 위한 조치	로그 수집 및 위·변조방지솔루션
령 30조2항: 개인정보처리자가 안전성확보를 위한 시스템 구축	고유 식별번호 외 인증수단
	방화벽, 침입탐지시스템, VPN, 망분리
	패치, 백신 프로그램
	SOC 또는 물리보안 영역

적하는 DB complex에 변동되는 DB구성 요소를 전송, 업데이트하는 Super DB를 제공하는 방식. 컴퓨터에 의하여 미리 결정된 특성이나 불법행위의 모형에 특정한 개인이 얼마나 가까운지를 평가하기 위하여 여러 개의 분리된 데이터항목을 상호 연결시킴. 이것은 통계적으로 비슷하게 나타난 다른 사람의 과거행태를 기초로 특정한 개인을 판단하는 것인데, 과거의 조사 및 예방적인 차원의 감시활동에 이용함. (4) Data matching; DB를 보유기관에 그대로 두고 대조할 DB를 대조될 DB와대조하여 목적을 달성하는 시스템 방식. 2개의 다른 기록시스템 속에 동일한 기록이 있는 것을 발견하기 위해서 컴퓨터처리에 의한 데이터비교(예; 여권전산망에서 여권신청자의 신청항목을 주민DB에 보내어 그 항목의 진위여부를 회신 받음).

재식별되는 것을 방지하기 위해서는 개인 식별자 중에서 어떤 식별자를 제거해야 되는지, 어떤 방법으로 익명화 할 것인지에 대한 논의가 있어야 한다. 이런 경우에 대해서는 개인정보보호법 제37조에 명시된 요구사항, 즉 정보주체가 개인정보의 처리정지에 대한 요구를 할 수 있음을 주목할 필요가 있다. 바로 이 부분에서 이차 활용을 통해 달성하고자 하는 이익과 개인식별이 되는 정보의 활용으로 인한 정보주체의 피해 간 이익형량을 수행해야 할 필요가 생긴다. 하지만 삭제를 요구하기 위해서는 적어도 정보주체는 자신의 정보가 어떤 목적으로 이차 활용되는지를 우선 고지 받아야 하므로 이러한 논의과정에 정보주체가 배제될 수 없는 것은 당연하다.

3.3.4 심의·의결절차의 문제점

개인정보보호를 언급하는 법제들에서 설립이 언급되고 있는 감독기구가 추상적인 원칙에 머물지 않기 위해서는 그 집행과 실효성을 담보할 수 있는 보호기구의 감시기능과 시정조치기능, 피해자 구제장치가 중요하다.[83]

개인정보의 목적 외 이용과 제3자 제공은 개인정보보호위원회의 심의·의결을 거쳐야 한다.[84] 개인정보보호위원회는 개인정보보호에 관하여 심의·의결하는 대통령 소속의 행정기관으로서, 공공기관의 개인정보 침해 등에 대한 시정 조치를 권고 할 수 있다. 개인정보 침해 여부의 판단 근거 조항으로서 대부분 개인정보

83) 서계원, 2005, “정보프라이버시와 개인정보의 보호”, 세계헌법연구 11권 1호: 223면.

84) 개인정보보호법 제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사항을 심의·의결하기 위하여 대통령 소속으로 개인정보 보호위원회(이하 "보호위원회"라 한다)를 둔다. 보호위원회는 그 권한에 속하는 업무를 독립하여 수행한다 ; 제8조(보호위원회의 기능 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다. 3. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항. 6. 제33조제3항에 따른 영향평가 결과에 관한 사항.

보호법 제18조 제2항의 적용 여부를 따지게 되는데, 개인정보를 청구하는 것이 적법한지, 제공하거나 제공받기 위하여 개인정보처리를 함으로써 개인정보호보법의 목적을 충족시키는지에 관한 것이다.

말하자면, 공공정보 제공을 요청 받은 공공기관은 소관 업무에 따라 구체적으로 어떤 특별 법률에 근거를 둘 것인지를 판단하고, 수집하는 기관이 아닌 제3자의 손에 개인정보가 들어갔을 경우 정보주체의 이익에 침해가 되는지를 판단한다. 여기서 침해의 기준은 공공기관 내부의 개인정보처리자의 정보처리에 관한 것이고, 개인정보처리가 곧 정보주체의 이익 보호라고 요약할 수 있다. 그러나 최근 제정된 '공공데이터의 제공 및 이용활성화에 관한 법률'에 따르면, 개인정보보호위원회의 제공여부를 판단하는 개인정보보호법을 적용하여 제공 부적합으로 판정된 정보라도 공개 대상일 수 있다. 동 법률에서는 공공기관이 공표를 목적으로 작성하거나 취득한 정보는 비공개대상에서 예외로 삼고 있고, 동 법률이 우선 적용되기 때문이다.

개인정보보호위원회가 이익형량의 근거로 하는 일반법으로서의 개인정보보호법의 적용이 배제되고, 특별법의 입법목적에 맞도록 공익을 위한 이차활용이 흠결 없이 이루어지려면, 무엇보다 개인정보보호위원회의 이러한 판단에 공익과 사적 권리의 행사에 대한 균형점을 찾을 수 있는 제도의 시행방법과 절차가 보완되어야 할 것이다.

3.4 공공정보의 이차 활용과 보호의 균형

공공정보를 이차 활용하여 여러 서비스를 개발하거나 시행하기 위해서는, 공공기관이 원래의 목적대로 수집한 원시자료를 통합하여 분석할 수 있는 정보통신

기술이 필요하다. 이 때의 기술은 공공데이터베이스에 있는 요청된 정보를 승인하고 전송해 주는 기술로서 최대한 프라이버시침해가 되지 않도록 정보를 제공하고, 전송된 정보를 모아서 프라이버시침해가 되지 않도록 분석하는 기술이다. 그리고 전송하는 정보는 익명 처리되어 누구에 관한 정보인지 식별이 안 되도록 해야 한다. 법에서 일컫는 개인정보에는 속하지 않는 정보를 제공할 수 있기 때문이다.[85]

그런데, 이차 활용의 특징은 어느 기관으로부터 원시정보를 제공받는지 상관없이 통계를 위하여 특정한 요구에 의해 가공되거나 구조화된 정보를 사용하게 된다는 것이다. 이차 활용을 하는 사람들에게 활용가치가 높은 정보는 유용성이 높은 정보이기 때문이다.[86] 이러한 유용성이 높은 정보는 그만큼 프라이버시의 침해위험도 높다.

그림 5에서 X 축은 정보의 유용성을 나타내며 Y축은 프라이버시가 침해당할 수 있는 위험도를 나타낸다. A, B 및 C는 데이터의 임의의 점을 나타내고, C는 거의 프라이버시가 보호되지 않는 원시데이터다.[87] 공공정보를 요청한 제3자는 가능하면 개인정보보호법의 테두리 안에서 익명화가 되어 있으면서도 가능하면 높은 유용성을 가지는 범위(Z)의 정보를 선택하려고 할 것이다. 즉 점선으로 표시된 제한선 내에서 적절하게 익명화된 정보를 얻고자 할 것이다. 그러나 중요한 것은 완전히 익명화된 정보는 유용성이 낮아지고, 익명화는 이차 활용 시 재식별이 될 수 있다는 점이다.

---

85) 황인호, 2002, "개인정보보호제도에서의 규제에 관한 연구", 공법연구, 제30집 제4호: 237면.

86) George T. Duncan, *et al.* 2001, "Disclosure Risk vs. Data Utility", National Institute of Statistical Sciences, Carnegie Mellon University: pp. 1-31; High data utility is analytically valid data, so faithful in critical ways to the original data; low disclosure risk is safe data, so confidentiality is protected.

87) 박원환, 황조연, 2004, "통계자료의 비밀보호를 위한 익명화 방법들", 통계연구, 제9권 제2호: 153-154면.

이렇게 공공정보의 이차 활용에는 아이러니가 있다. 즉 정보를 이용하고자 하는 사람은 유용성이 높은 정보를 얻고자 할 것이고, 제공하는 공공기관은 프라이버시를 보호하기 위하여 익명성이 높은 정보를 주려고 할 것이다.

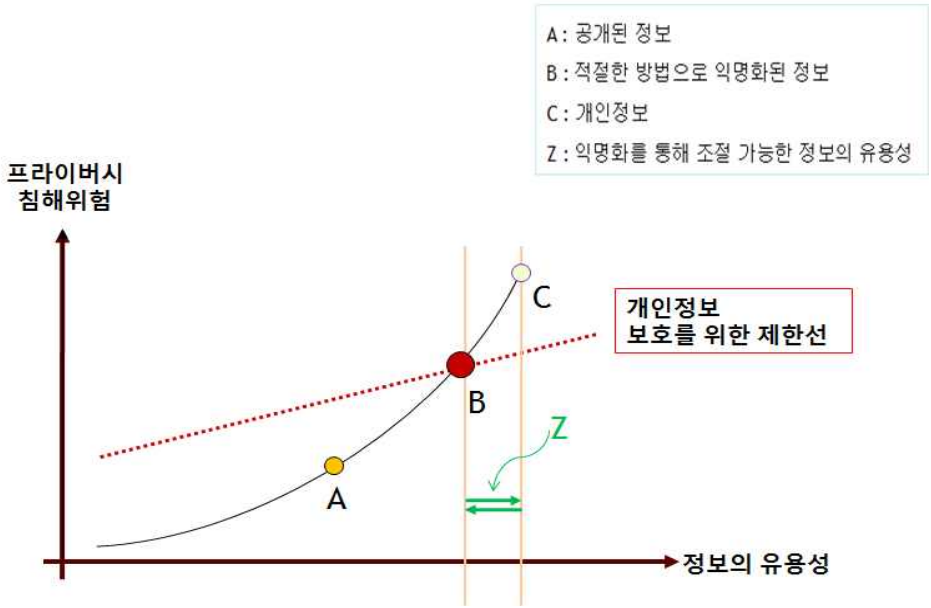

그림 5. 정보의 유용성과 프라이버시 침해위험과의 관계

이러한 정보의 유용성과 프라이버시 침해위험과의 긴장관계를 감안하면, 익명화[88]의 기술과 익명화 처리를 하는 개인정보처리자의 역할은 똑같이 중요하다.[89]

88) 개인정보보호법 제2조 제19항; 개인식별 정보를 영구적으로 삭제하거나, 개인식별 정보의 전부 또는 일부를 해당기관의 고유 식별 번호로 대체하는 것을 말한다.

89) Anne Cambon-Thomsen, 2004, "The Social and Cultural Issues of Post-Genomic Human Biobanks", Nature Reviews Genetics 5: p. 869; ①Traceable or coded. A code is attached to them and the correspondence between code and identity is physically separated from sample and data. A limited number of people can connect the code to the identity. ② Encrypted. There is a further level of protection through encryption (that is, the code is transformed into several characters that are linked to the code with the intervention of a third party). This third party intervention will then be required to trace individual

예를 들면, 동일한 속성의 데이터 값은 식별자와 준 식별자를 익명화하여도 비슷한 값의 조합으로 개인이 식별될 수가 있다. 말하자면 이차 활용을 통하여 익명화된 정보가 재식별되는 경우가 발생할 수 있는데, 그림 6에서 보는 바와 같이 링크를 통하여 재식별이 되는 환자명과 질병 명을 확인할 수 있다.

그림 6. 익명화와 linkage를 통한 재식별의 예

따라서 개인정보 처리자가 어떤 기술방법을 적용하느냐가 중요하며, 이러한 측면에서 정보주체, 공공기관 정보처리 담당자, 공공정보 이차 활용자들의 입장을 함께 논의할 수 있는 구체적인 정보처리 과정과 운영체계를 새롭게 마련할 필요가 있다. 최근에는 항목별 속성 값을 일반화시켜 재식별을 방지하는 등의 익명화 방법을 논의하고 실제 적용한다.[90] 이는 공공정보의 이차 활용에 대하여

identity. ③Anonymized. The link has been irreversibly cut between sample/data and the individual identity.

90) anonymization의 방법으로 데이터의 속성을 식별자, 민감정보, 준식별자로 분류하여 'k'명의 준 식별자 정보를 일반화 하는 k-anonymization, 비구조화 정보를 익명화하는 패턴인식이나 기계학습, 가명화 등이 있다.

별도의 규범적인 한계설정을 통하여 정보주체의 권리를 보호한다는 의미이다. 동시에 개인정보보호법에서 개인정보보호 정도를 민감정도[91]에 따라 차별화하여 보호하는 것처럼, 이차 활용에서도 어떤 정보를 어떤 방법으로 활용할 수 있는지에 대해서 차별화하여 언급해 줄 필요가 있다는 것이다.

앞장에서 언급한 바와 같이, 개인정보자기결정권은 자신에 관한 정보의 흐름을 자율적으로 형성할 수 있도록 한다는 점에서 헌법상의 권리라고 할 수 있다. 전자정부[92]에서는 이러한 개인의 권리와 공공정보를 이차 활용하기 위해서 강조되는 효율성이나 목적합리성이 긴장 관계를 갖게 된다. 다시 말하면, 개인정보의 '수탁자(fiduciary)'로서의 정부는 고도로 발전된 정보통신기술을 활용하여 맡겨진 정보의 개방과 이차 활용을 촉진시키려 하는 반면, 개인정보를 맡긴 정보주체에게 수탁한 그 정보를 제어하는 권한을 준 것이다. 이른바 개인정보보호의 역설이 발생하는 것이다.[93] 이러한 긴장은 입법 목적에서부터 발생한다.

개인정보자기결정권은 양도하거나 양보할 수 없는 기본적 가치임에는 틀림없으나

---

91) 개인정보보호법 제23조; 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.; 개인정보보호법 시행령 제18조; 법 제23조 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. 1. 유전자검사 등의 결과로 얻어진 유전정보 2.「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보.

92) 전자정부법 제2조; 전자정부란 정보기술을 활용하여 행정기관 및 공공기관(이하 "행정기관 등"이라 한다)의 업무를 전자화하여 행정기관 등의 상호 간의 행정업무 및 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다.

93) Patricia A. Norberg, Daniel R. Horne and David A. Horne, 2007, "The privacy paradox: Personal information disclosure intentions versus behaviors", Journal of Consumer Affairs Volume 41, Issue 1: pp. 100-126.

절대적인 가치가 아닌 상대적인 가치다. 왜냐하면 사생활 영역을 벗어난 부분이나 공적 영역에서 자연스럽게 혹은 자발적으로 노출되는 개인정보도 있기 때문이다. 그리고 자신에 관한 정보라 할지라도 정보주체가 무제한적으로 지배할 수 있는 것이 아니고 법률에서 정한 일정한 한계도 존재하기 때문이다. 요컨대, 개인정보보호의 역설을 극복하기 위해서는 사적 권리로서 개인정보자기결정권과 공적 필요성으로서 공공정보의 이차 활용간 적절한 '균형(equilibrium)'을 발견하는 작업이 필요하다.

최근에는 공공기관이 수집·보관·관리하는 개인정보와 대규모 데이터베이스에 집적된 생체정보, 의료기관에서 생성된 의료정보를 모두 이차 활용하는 추세다. 이러한 생체·의료정보는 법률에서는 '민감정보'로 구별하여 쓴다. 그리고 일반적인 개인정보의 보호와는 다른 수준의 보호에 대한 규정이 있다.

다음 장에서는 민감정보로서 생체·의료정보의 이차 활용에 대한 요구와 그 활용을 제한하는 법익간의 균형점을 모색해 본다.

제4장 생체·의료정보 이차 활용과 보호

생체·의료정보는 인간유전체 연구[94]나 의생명과학연구[95]등 효율적인 학술연구 목적으로 이차 활용된다.[96] 의생명과학연구는 일반적인 개인정보와 유전정보, 인체유래물 정보, 건강정보를 모두 이용한다. 학술연구자 대부분은 생체·의료정보가 수집·보관되어 있는 공공기관에 정보제공을 요청한다. 그러나 요청하는 모든 연구자가 원하는 정보를 얻어 이차 활용을 하지는 못하고 있다. 왜냐하면 대개는 개인정보보호법에서 규정하는 개인 식별자를 제거한 정보를 제공받으므로 이차 활용성이 떨어지기 때문이다. 또한 이차 활용을 하여 개인이 식별되는 것을 염려하여 아예 시도조차 하지 못하기도 한다.

생체·의료정보를 이차 활용하는 인간 대상 연구의 근거가 되는 '생명윤리 및 안전에 관한 법률'에서도 정보주체의 사전 서면동의를 얻어야만 연구를 할 수 있도록 하고 있다. 하지만 연구자들이 직접 서면 동의를 구할 정보주체가 너무 많거나, 정보주체의 사망이나 이사 등으로 동의를 받을 수 없는 경우가 있다. 이런 경우, 연구를 심의하는 기관윤리위원회에서 서면동의 면제에 대한 사항을 심의하는 것으로 법적 장치를 마련하고 있다.

---

94) 1990년, 미국 국립보건원(NIH)은 아래 전 세계 수십 개 연구기관이 공동으로 참여한 '인간유전체연구(Human Genome Project)'를 진행하였다. 연구의 기대성과는 인간유전체의 염기서열을 완전히 해독하고 이를 이용하여 모든 질병의 원인을 미리 파악한다면 질병예방 및 진단, 치료신약 및 치료기술의 개발이었다. 그리고 2003년, 미국 국립보건원은 인간유전체 염기서열의 완전해독결과를 발표하였다.

95) 의생명과학연구는 생명공학 및 생물학 연구와 의학연구를 지칭한다. 기초생명과학의 지식으로부터 새로운 진단법과 치료법을 개발하고 적용하는 바이오산업의 성향을 띠는 연구로서 환경과 유전 등 질병의 인과 관계를 명확히 밝히고, 국민에게 양질의 의료를 제공하고, 치료비용을 낮추고, 치료기술의 타당성을 평가하고, 어떤 예방 방법이 더 적절할지, 어떻게 의료자원을 이용할지에 대한 정책적 판단을 하기 위한 근거마련 연구 등이 있다.

96) David A. Wheeler et al. 2008, "The complete genome of an individual by massively parallel DNA sequencing", Nature 452: pp. 872-876.

의생명과학연구를 하기 위해서 필요한 정보의 양과 그 종류도 많아졌지만, 이러한 정보를 수집·관리·분석하는 방법도 다양해졌다. 따라서 정보주체의 사적 권리 보호의 기준도 변화할 필요가 있다. 이 장에서는 현행법이 생체·의료정보의 이차 활용만 저해하고, 정작 법에서 보호하려고 했던 프라이버시는 침해되는 것은 아닌지 검토하고자 한다. 민감정보를 다루는 의생명과학연구는 정보학적으로 효율적인 분석방법론[97]만큼이나 정보주체의 권리와 공익에 대하여 깊은 이해와 이를 절차화한 법제도적인 개입이 필요할 것이기 때문이다.

4.1 생체・의료정보의 개념

본 논문에서 생체정보와 의료정보를 함께 다루고자 하는 이유는 법적 대상으로서 민감정보라는 공통점이 있기 때문이다. 또한 DNA와 의료정보를 활용하여 맞춤형 의료시대를 대비하고, 국민의 건강과 복지 수준향상을 목표로 하는 융합연구가 우리나라의 보건산업의 큰 방향이 되었기 때문이다.[98]

이와 더불어 전 국민의 영양조사 결과를 수집·관리하고, 증가하는 대규모의 인체유래물의 수집·관리 및 유전체 연구를 위한 데이터관리를 위해 공공데이터베이스의 가용성에 대한 의존은 더 많아질 것이기 때문이다.[99] 우선 현행 법률에서 정의하는 생체정보와 의료정보의 뜻을 살펴본다.

---

97) ENCODE Project Consortium, 2007, “Identification and analysis of functional elements in 1% of the human genome by the ENCODE pilot project”, Nature 447: pp. 799-816.

98) 미래창조과학부 외, 2014, 생명공학육성시행계획, Bio-vision 2016: 47-102면.

99) Kate R. Rosenbloom *et al.* 2009, "ENCODE whole-genome data in the UCSC Genome Browser", Nucleic Acids Research. Volume 38: pp. 620-625.

4.1.1 생체정보의 개념

‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’ 등 관계법령의 개인정보 보호 원칙을 토대로 마련된 한국인터넷진흥원의「바이오정보 보호 가이드라인」에 의하면, 생체정보란 지문·얼굴·홍채·정맥·음성·서명 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다. 그런데 개인정보의 정의 내에는 생체특성에 관한 정보가 포함되어 있다. 즉 개인정보는 부호, 문자, 음성, 음향이나 생체 특성 등에 관한 정보를 망라하고,[100] 해당 정보만으로는 특정개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.[101]

또한 ‘보건의료와 관련한 지시 또는 부호, 숫자, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료’[102]라는 정의에 의하면, 질환 검사를 통해 얻을 수 있는 개인에 관한 정보까지도 개인정보이다. 적어도 이론적으로 한 방울의 피는 특정치료에 대한 반응을 예상하는데 도움을 주고, 질병의 소인에 대한 귀중한 정보를 제공하며, 질병 메커니즘과 병인에 대한 유전자의 역할 연구를 돕는다. 그리고 생물학적 검체를 장기간 보관할 때, 유전자형-표현형 상관관계에 대해 심도 있는 이해를 추구하는 연구자들에게 귀중한 정보를 제공한다.

또한 생체인식 기술이 발전함에 따라 손 모양, 얼굴, 홍채, 지문, 정맥, 손금 등 신체적 특징뿐만 아니라 행동적 특징까지도 생체정보의 요소가 될 수 있다. 예컨대, 서명이나 필체, 음성, 걸음걸이 등이다.

최근 유전자 서열 및 변이 정보를 추출하여 개인별 다양한 질병진단에 이차 활용하고 있다. 개인특성에 맞는 처방과 치료를 목표로 유전체를 분석하는 것이다.

---

100) 정보통신망이용촉진 및 정보보호 등에 관한 법률 제2조 6호.

101) 전자서명법 제2조 13호.

102) 보건의료기본법 제3조 6호.

즉 유전자염기서열(SNPs)분석은 질병의 위험을 평가하고, 친자확인에 사용되며, 개인이 어떤 환경과 물질에 취약한 지를 예측하는 도구로 사용되고 있다. 본 논문에서는 염기서열 정보(genomic sequence data)와 유전자염기서열 정보(Single Nucleotide Polymorphism; SNP data)까지 생체정보로 본다.

4.1.2 의료정보의 개념

의료정보와 관련된 법조문으로는 '의료법' 제22조의 진료기록부(조산기록부, 간호기록부, 그 밖의 진료에 관한 기록)와 '의료법시행령 제22조'에 의료정보 시스템 사업과 관련한 1. 전자의무기록을 작성·관리하기 위한 시스템의 개발·운영사업, 2. 전자처방전을 작성·관리하기 위한 시스템의 개발·운영사업, 3. 영상기록을 저장·전송하기 위한 시스템의 개발·운영사업에 관한 규정이 있다. 이 조문을 토대로 진료기록부등, 전자의무기록, 전자처방전, 영상기록을 '의료정보'라고 정의할 수 있다.[103]

판례에서는 '의료 내지 진료라는 특정 상황에서 환자의 상태와 치료경과 등 의료행위에 관한 사항과 소견'[104]도 의료정보로 본다. 광의의 의료정보의 개념에는 의료기관에서 생성되는 병원행정·경영, 의학교육, 국가보건의료정책과 보건의료 사업 분야 등의 과정에서 생성되는 정보 또한 포섭될 수 있다.

또한 의료법 제18조 및 제19조에서는 의사·치과의사·한의사는 직접 진료한 환자에게 처방전을 작성하여 교부할 의무를 부여하고 있는데, 이때 처방전은 전자서명이 기재된 전자처방전 형태로 작성·발송할 수 있도록 하고 있다. 따라서

---

103) 임진희 외, 2012, "의무기록관리의 현황과 개선방안", 정보관리학회지, 제29권 제3호: 259-285면 참조; 우리나라는 2003년 5월 국립대학병원이 전자의무기록을 도입하여, 2010년 현재, 3차 의료기관 44곳 중 77.3%가 전자의무기록을 사용하고 있다.

104) 대법원 1998. 1. 23. 선고 97도 2124 판결.

의무기록상 보건의료정보의 형식적인 종류는 의료법시행규칙 제14조(의무기록의 기재사항) 내지 제15조(의무기록의 보존연한)에서 정하는 내용과 같으며, 구체적으로는 진료기록부·조산기록부·간호기록부와 처방전·수술기록·검사소견기록·방사선사진 및 그 소견서·환자명부·진단서 등의 부본 등도 포함된다.

이밖에 인쇄매체 형태의 진료기록 및 처방전 이외에 이들을 전자적 장치를 이용하여 디지털화시킨 디지털보건의료정보(digital health & medical information)[105]가 있다. 그리고 건강보험자들의 의료보험 자료를 전산화하여 '전자 자료 교환(Electronic Data Interchange; EDI)' 정보도 대표적인 의료정보라고 할 수 있다.

미국의 HIPAA(Health Insurance Portability and Accountability Act)에서는 개인으로부터 수집된 통계정보를 의료정보에 포함하고, 특히 '개인식별 건강정보'라고 별도로 정의하고 있다. 즉, 의료공급자, 의료보험, 고용주 또는 의료정보센터(health care clearinghouse)에 의해 수신되거나 생성된 정보로서 개인의 과거, 현재, 또는 미래의 신체적, 정신적 건강관리와 관련된 정보, 합리적인 판단에 의해 개인을 식별하는데 사용될 수 있다고 간주되는 정보를 건강정보라고 정의한다.[106]

본 논문에서도 의료기관에서 생성·관리하고 있는 정보뿐만 아니라 의료보험 및 보험급여와 관련하여 공공기관에서 수집·관리하고 있는 의료이용 및 급여청구 정보도 의료정보라고 본다.

---

105) 진료차트 등 의무기록의 디지털화는 주로 다음과 같은 방법을 활용한다. ① 의료법 제23조에 따라 처음부터 전자서명이 기재된 전자의무기록형태로 작성으로서 자동처방전달시스템(order communication system; OCS), 검사정보자동화시스템(laboratory information system; LIS), 영상정보저장전달시스템(picture archiving & communication system; PACS)을 통하여 보건의료정보를 디지털화 할 수 있다. ② 의료법시행규칙 제15조 제2항과 제3항에 따라 인쇄매체 형태의 진료기록을 마이크로필름이나 광 디스크 등으로 원본대로 보존하는 방법이 있다.

106) Standards for Privacy of Individually Identifiable Health Information 45 CFR Parts §160 and 164.

4.1.3 통합개념으로서 생체·의료정보의 개념

‘생명윤리 및 안전에 관한 법률’ 제2조에서 ‘개인식별정보’란 연구대상자와 배아·난자·정자 또는 인체유래물의 기증자(이하 “연구대상자등”이라 한다)의 성명·주민등록번호 등 개인을 식별할 수 있는 정보를 말한다. ‘개인정보’란 개인식별정보, 유전정보 또는 건강에 관한 정보 등 개인에 관한 정보를 말한다. 동 법률에서는 생체 정보와 의료정보를 함께 사용하고 있다. 위와 같은 법률적 정의를 종합해 보면,「개인을 식별할 수 있는 정보와 인체유래물,[107] 유전정보, 전자진료기록, 의료행위로부터 얻어진 개인정보」의 개념이 모두 들어 있다. 따라서 본 논문에서 다루는 생체·의료정보란 ‘인체 유래물, 유전정보, 유전자 검사정보, 전자의무기록, 의료기기로부터 수집되는 개인식별정보’를 뜻한다.

변화하는 의료기술과 의료서비스, 의료서비스의 전달환경에서 생성되고 전송되는 생체정보까지도 병원에서 생성된 의료정보와 함께 활용될 수 있기 때문에 생체·의료정보의 개념은 확대가능하다. 몇 가지 사례를 들어보자. 의료기관별 전자의무기록에 기술적 호환성을 갖추어 여러 의료기관에서 생성되는 개인의 건강관련기록(electronic health record, EHR)을 네트워크화 하는 추세다. 또한 현장진료와 병원에서의 협진으로 이어지는 원격의료(telemedicine)도 그 필요성이 높아지자 사고나 재난 현장에서 직접 혈압, 맥박수, 호흡수, 체온, 산소포화도, 심전도, 외상초음파, 혈액성분 분석 등 생체정보를 측정할 수 있는 기술이 발전하고 있다. 그리고 소형화 되고 휴대할 수 있는 기기를 이용하여 생체정보를 획득하는 것도 더 저렴한 비용으로 용이해지고 있다.

---

107) 생명윤리 및 안전에 관한 법률 제2조 제11항; "인체유래물"(人體由來物)이란 인체로부터 수집하거나 채취한 조직·세포·혈액·체액 등 인체 구성물 또는 이들로부터 분리된 혈청, 혈장, 염색체, DNA(Deoxyribonucleic acid), RNA(Ribonucleic acid), 단백질 등을 말한다.

시간과 공간의 제약을 최소화하여 거동할 수 없는 환자들에게 병원에서와 같은 건강 및 질환 관리가 가능하도록 하는 u-헬스(Ubiquitous healthcare), 모바일원격진료(m-telemedicine)등도 질환자와 환자 보호자, 건강한 사람들에게서 폭넓게 그 유용성을 인정받고 있어, 질병 진단 및 건강 체크를 병원에 직접 방문하지 않고 집에서도 할 수 있는 바이오칩이나 센서 기술이 개발되었다. 그리고 정보통신기술과 융합으로 생체·의료정보를 병원 밖에서 병원에 보낼 수 있게 된 것이다. 자가진단에서 측정된 고혈압 수치가 네트워크를 통해 병원에서 그 정보가 수집되고 병원에 있던 진료정보와 함께 관리될 수도 있다.

그림 7은 의료기술 현대화에 따라 생체정보와 의료정보가 함께 활용되는 가능성이 더 증가하고, 의료 서비스의 내용과 제공방식도 변화하고 있음을 도식화한 것이다. 108)

그림 7. 생체-의료정보의 통합기술과 의료서비스의 변화

108) 과학기술부, 2002. 국가기술지도(NTRM), 비전II 건강한 생명사회 지향 제2권: 115-120면.

이차 활용의 측면에서는 생체정보와 의료정보를 한 군데의 데이터베이스 혹은 시스템에서 관리하며, 인간유전체 정보와 유기적인 연동을 통하여 ENCODE Project로 대표되는 기능연구, 주요 질환과 관련 된 후성 유전체 연구 등을 포함하는 유전체 연구 및 다년간 코호트 연구 등이 연구가 가능해진 것이다. 특히 유전체 연구에 있어서 중요한 분야중 하나가 메타정보를 포함한 데이터베이스이다.
이러한 데이터베이스의 특징 중의 하나가 민간과 공공기관을 망라하여 다양한 기관에서 수집·보관되어 있는 유전체 정보를 연계하고, 연구 자원을 공유하는 것이다.[109] 이와 같이 생체정보와 의료정보가 통합되어 관리될 수 있는 기술의 발전과 시스템의 개발 방향을 고려하여 본 논문에서는 두 개념을 하나로 묶어 사용하려고 한다.

4.2 공공정보로서 이차 활용되는 생체・의료정보의 특성

본 연구에서는 공공정보이기 때문에 이차 활용대상은 되지만 민감정보라는 특수성을 동시에 지니고 있는 생체·의료정보의 다음과 같은 특성에 주목하였다.

첫째, 공공기관 간에는 동의 없이 사용할 수 있다.

2013년 우리나라에서 개최된 UN 공공행정포럼에서는 우리나라의 공공정보 공동이용에 대한 사례가 소개되었다.[110] 여권발급의 경우인데, 여권신청을 하기 위해서 한 가지 신청서와 본인확인만 되면, 한 곳에서 행정담당자가 필요한 정보를 온라인에서 조회하여 발급할 수 있게 된 것이다(그림 8). 네 가지 종류의 일곱 장의 서류가 필요하여 개인정보를 별도로 기관별로 수집해야 했던 행정업무가 공공정보 공동이용을 통하여 개인정보가 포함된 공공정보를 한곳에서 관리하고,

109) Kelly A. Frazer1. *et al.,* 2009, "Human genetic variation and its contribution to complex traits", Nature Reviews Genetics 10: pp. 241-251.

110) United Nations Public Service Forum, 2013, 24th-27th June, Seoul.

공동으로 활용함으로써 가능해진 사례이다.

그림 8. 개인정보가 포함된 공공정보 공동 이용의 예

이 밖에 조세, 4대 보험, 무역, 국가기록물 관리, 국가통계, 국가정책조사, 국토 이용, 건축 등 다양한 분야에서 원시자료로서 개인정보가 포함된 공공정보는 공동 이용되고 있으며 이때 정보주체의 동의는 면제된다.[111]

하지만 정보주체의 기본적 인권을 현저하게 침해할 우려가 있는 내용을 포함하는 민감정보[112]는 수집할 수 없으며, 원칙적으로 제3자에 의한 처리 자체가 제한된다. 대부분의 이차 활용은 학술 연구에서 행해지며, 민감정보의 수집과는 별도로 다른 법률을 적용하며, 최소한의 개인정보 수집, 최소한의 활용의 입증책임은 공공기관이 갖는 것이 필요하다.[113]

111) 공공데이터의 제공 및 이용 활성화에 관한 법률 제2조, 제3조, 제4조, 제17조; 전자정부법 제12조.

112) 우리나라의 개인정보보호법 제23조. 영국의 데이터보호법 제2조, 유럽연합의 Directive 95/46/EC 제8조.

둘째, 공익목적으로 이차 활용될 수 있다.

한국 인체자원 은행에서는 수집된 인체자원을 이차 활용을 위해 연구자들에게 이를 분양하고 있다.[114] 우리나라 질병관리본부의 '한국 인체자원은행'에서 수집·관리되는 인체자원은 종류별로 모두 백이십오만 명을 훌쩍 넘는다(그림 9).[115]

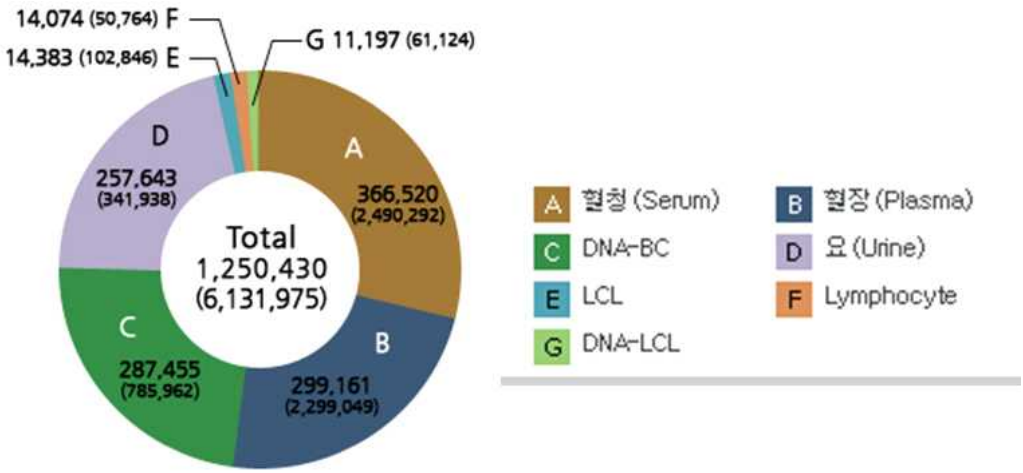

그림 9. 한국인 인체자원 종류별 수집현황

인체유래물이 학술 연구에 활용될 수 있는 배경은 공여된 인체 유래물들이 비록 개인으로부터 유래되었지만, 신뢰할 수 있는 기관에서 공익을 위해 사용할 수 있는 일종의 공공재(public good)로 보아야 한다는 입장에서 그 정당성을 찾을 수 있다. 우리나라뿐만 아니라 여러 국가가 국민의 건강과 국제적 경쟁력을 확보하기 위한

113) Timothy Caulfield, *et al.,* 2008. "Research ethics recommendations for whole-genome research: consensus statement." PLoS biology No. 6(3): p. 73; Corrigan, Oonagh, and Richard Tutton. 2004. Genetic databases: Socio-ethical issues in the collection and use of DNA, Kentucky, Routledge: pp. 172-192.

114) 한국인체자원은행사업. http://kbn.cdc.go.kr/kbn/com/ntw/viewHospKbn.do

115) 국립중앙인체자원은행 보유자원 현황. 2012. 12.31. 기준 http://kbn.cdc.go.kr/kbn/com/sts/viewCollStatic.do 참조.

중대한 분야로 인식하여 인간유전체 연구를 진행하고 있다.[116] 국내의 경우 인간 유전체 연구 분야에서는 한국인 특이적인 유전질환에 관한 연구, 인간 질환 및 노화 연구가 생체·의료정보를 이차 활용하는 대표적인 연구라고 할 수 있다. 이러한 정보의 융·복합 연구는 질환과 유전자의 상관관계를 찾아 질병을 예방하기도 하고, 개인 유전자 정보를 전자건강기록과 연계해 통합 관리함으로써 더 좋은 약물과 치료기법을 도출하기도 한다. 인간 유전체 연구의 방향은 임상정보를 결합한 질환 치료 및 개인 맞춤형 의료로 진화 하고 있기 때문에 점점 유전체자원의 확보와 시스템의 연계방안을 위해 공공기관간의 협력은 현실적인 요청에 직면해 있고 할 수 있다.

한편 전 국민건강보험 제도를 실시하고 있는 우리나라는 국민의 건강보험 청구 자료가 건강보험심사평가원에 수집·보관되어 있으며, 학술연구를 위하여 제공된다. 그러나 기관마다 자료원의 개발 목적이 다르고 규모와 특성도 다양하여 연구자들은 이들 기관에서 원시자료를 수집한 후, 다시 연구목적에 맞게 재가공하여 분석하고 있다. 한국 중앙 암 등록 본부에 암 등록 통계자료, 질병관리본부에 국민건강영양조사 자료 등이 수집·관리되고 있고, 학술연구를 위해 제공된다. 국민건강보험공단, 보건복지부, 통계청, 한국보건사회연구원 등 보건의료분야에서 이차 활용에 필요한 자료가 수집되어 있다(표4).[117]

---

116) 최근 영국 정부가 내놓은 '10만 게놈 프로젝트'는 10만 명에 달하는 암 환자는 물론 유전질환 환자 혈액 샘플을 채취하고, 유전정보가 활용되는 연구이다. 영국은 2017년까지 DNA 검사에 3억 파운드를 지원한다. The Wall Street Journal, 2014. 7. 31; UK to Become World Number One in DNA Testing with Plan to Revolutionise Fight Against Cancer and Rare Diseases 참조.
http://online.wsj.com/article/PR-CO-20140731-918370.html

117) 국내 보건의료 이차자료원 활용. 2013. NECA 연구방법 시리즈 5. 서울, 한국보건의료연구원: 3-5면 참조.

표 4. 국내 생체·의료정보의 수집 기관 및 목적

담당기관	이차 활용 가능한 자료원명	수집 목적	수집 주기
건강보험심사 평가원	건강보험청구자료	요양급여심사 및 요양급여 적정성 평가를 위한 청구자료	매년
국립암센터	중앙암등록자료	전국단위의 암 발생 자료를 구축하는 등록자료	매년
국민건강보험 공단	국민건강보험공단 건강검진자료	공공건강검진 자료	매년
통계청	통계청 사망원인자료	정확한 사망원인구조 파악	매년
보건복지부	국민구강건강실태조사	국가차원의 체계적인 구강보건 사업목표 개발과 사업계획 및 구강보건사업 우선순위 결정에 필요한 기초자료	3년
질병관리본부	국민건강영양조사	국민의 건강수준, 건강관련 의식 및 행태, 식품 및 영양섭취 실태에 대한 국가 및 시·도 단위의 통계산출	매년
	지역사회건강조사	근거 중심의 보건사업 수행기반 마련, 지역 간 비교 가능한 지표조사	매년
	청소년건강행태 온라인조사	국내 청소년의 건강행태 통계 산출, 청소년 건강증진 사업의 기획 및 평가	매년
	퇴원손상심층조사	의료기관 퇴원환자에 대한 국가 단위의 보건의료 통계생산	매년
	한국인유전체역학조사	40-69세 일반인구 코호트구축 건강 및 생활습관 관련 설문조사와 검진 역학 자료와 혈액, 소변, 유전체 등의 생체시료를 수집, 만성질환과 관련한 지표	매년
한국보건사회 연구원	노인실태조사	노인생활 현황과 건강 및 복지상태의 변화 추이관찰	3년
	장애인실태조사	우리나라 장애들의 생활실태 및 복지서비스 욕구 등을 파악	3년
	전국출산력 및 가족보건 복지실태조사	인구 및 가족보건복지 정책 수립에 필요한 기초자료	3년
	영아모성사망조사	모성사망의 수준 및 원인에 대한 통계생산으로 모자보건 증진을 위한 기초자료	매년
	환자조사	전국 의료기관을 대상으로 일정기간 동안 의료기관을 이용한 환자의 질병, 상해 양상과 의료이용 실태, 보건의료시설 및 인력파악	1년

셋째, 수집된 생체·의료정보는 진료행위에 직접 활용되기 보다는 제3자에 의해 다른 목적으로 활용된다.

생체·의료정보는 일반인이 습득하기도 어렵지만 설령 습득한다고 하더라도 그 자체만으로는 특정개인과 연관 지어 식별할 수 없지만, 공공기관 외부의 다른 정보와 linkage를 하는 이차 활용을 통해 식별될 수 있는 가능성이 내포되어 있다. 또한 건강정보들과는 달리 유전자 정보는 한 사람 이상에게 해당하거나 적용 가능하다. 게놈분석을 통해서 해당 인물의 부모, 형제·자매, 자녀, 그리고 다른 사람에 대한 정보도 확인할 수 있다. 이는 연구의 기존 주제나 근거정보 또는 검체를 제공한 개인이 아닌 사람들의 사생활 또는 비밀보장도 손상될 수 있다는 것을 뜻한다.

넷째, 생체·의료정보는 개인의 건강이나 질병에 관한 정보로서 '민감한 정보'로 분류되어 특별하게 보호된다.[118]

생체·의료정보는 의료인 및 의료기관과 환자 사이에서 이루어지는 진료행위라는 정보교환과정을 통해 생성된다. 따라서 의료인 및 의료기관과 환자 간의 의료계약을 시발점으로 생성되므로 사적인 성질을 가진다. 이러한 정보는 환자본인의 진료를 위해서 이용되었으며, 부분적으로는 의료인에 의하여 질병의 통계나 진단 및 치료방법의 효율성을 알아보기 위한 목적으로 사용되었다.

만약 생체정보가 도난당한다면, 이것은 폐기되는지 확인 할 수 없다. 이로 말미암아 평생 동안 낙인이나 차별로 이어질 수 있는 원인을 제공할 수 있고, 개인뿐만 아니라 그 가족이나 자손에까지 영향을 미친다.[119] 보다 광범위하게는,

---

118) Mary R. Anderlik and Mark A. Rothstein. 2001. "Privacy and confidentiality of genetic information: what rules for the new science?" Annual Review of Genomics and Human Genetics No. 2(1): pp. 401-433; 생체정보는 민감하여 차별이나 낙인, 보험 및 고용에 대한 불이익을 야기 할 수 있으며 정보주체뿐만 아니라 그 가계에도 마찬가지 우려가 있다.

119) UNESCO, 2003, "PUBLIC HEARINGS DAY on Human Genetic Data", International Bioethics Committee FINAL REPORT: pp. 1-49.

유전자 연구는 인종이나 민족 집단 같은 전체 하위 인구집단을 포괄하는 발견을 이끌 수 있다. 여기서 연구자와 연구기관은 '집단 사생활'이라는 개념에 대해 심각하게 고민할 필요성이 요구되며 유전자 연구의 계획, 관리, 그리고 유전자 연구결과 공개 시에는 공동체 구성원들도 포함시키는 단계를 고민해야한다.

본 논문은 생체·의료정보가 비록 공공정보라고 할지라도 일반적 공공정보와 달리 이차 활용을 꺼리는 이유를 위와 같은 특성에서 찾을 수 있다고 본다. 그리고 이차 활용을 할 수 밖에 없는 경우를 대비하여 이러한 특수성을 감안하여 필요한 법적 조치를 보완할 필요가 있다. 앞서 이론적 배경에서도 보았듯이 개인의 사적 권리가 온전히 개인만의 것이 아니며, 공익을 위해 제한받을 수 있다는 점을 감안하여 공공정보 중에서 생체·의료정보가 공익을 위하여 이차 활용되는 정당성을 찾는 것이다. 그 정당성으로부터 정보주체의 프라이버시를 보호하는 바람직한 법제도 개선방향이 나올 수 있을 것이다.

이제 구체적으로 이차 활용 자체를 제한함으로써 프라이버시가 보호되는 것인지, 아니면 안전하게 이차 활용하는 것이 정보주체에게 더 많은 이익이 있는 것인지를 그 쟁점을 통해 하나씩 살펴본다.

4.3 생체・의료정보의 이차 활용과 관련한 법적 쟁점

생체·의료정보를 이차 활용하기 위해서는 공공기관이 수집·관리하는 정보를 해당 기관에 요청하여야 한다. 원칙적으로 제3자에 의한 처리는 불가하지만 다른 법률에 근거를 둔다면 예외가 적용되는 점을 근거로 요청하는 것이다.[120]

120) 개인정보보호법 시행령 제18조(민감정보의 범위); 개인정보보호법 법 제23조 각 호 외의 부분 본문에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법제18조 제2항 제5호부터 제9호까지의 규정에 따라 다음 각 호의

예를 들면, ‘전자정부법’에서는 사전 동의 요건이 면제되는 예외적인 경우를 허용하는데, 이를 근거로 공공기관 간 정보공유가 가능하다.[121] 이렇게 공공정보에 대한 서면동의 면제로 인해 정보주체는 개인정보자기결정권을 행사할 수 없을 뿐만 아니라 어떤 목적의 공익을 위해 이차 활용되는지 알 수 있는 기회조차 가질 수 없다. 개인정보자기결정권을 통하여 민감정보를 보호하려는 법익을 충족시키고, 생체·의료정보의 이차 활용에 대해서도 철저하게 개인정보자기결정권을 관철하려면 예외적인 경우인 공익보다 더 긴절한 사적 권리의 보호가 요구되도록 법적 근거 제시가 이루어져야 할 것이다.

4.3.1 이차 활용을 위한 동의절차상의 쟁점

바이오뱅크(인체유래물 은행)에 모이는 인체유래물 및 관련 데이터베이스에 보관·관리되는 생체정보는 다른 공공기관의 의료정보와 함께 이차 활용되는 경우가 대부분이다. 또한 공공기관 밖에서 유입되는 생체 정보도 의생명과학 연구자들이 이차 활용하는 다른 공공정보 및 의료정보와 함께 쓰일 수 있다. 그런데 바이오뱅크에서 보관되고 사용하는 인체유래물이 시간이 경과된 후에

어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다. 1. 유전자검사 등의 결과로 얻어진 유전정보 2. 형의 실효 등에 관한 제2조제5호에 따른 범죄경력 자료에 해당하는 정보.

미국의 경우는「caBIG 데이터 공유」프레임워크에 명시되어있다; Data Sharing and Security Framework Fact Sheet, 2007. National Cancer Institute. National Committee for Vital Health Statistics (NCVHS).

121) 전자정부법 제42조 제2항 1. 정보주체의 생명 또는 신체를 보호하기 위하여 긴급하게 공동 이용할 필요가 있는 경우. 2. 법령에 따라 정보주체에게 의무를 부과하거나 권리·이익을 취소·철회하는 업무를 수행하기 위하여 공동이용이 불가피한 경우. 3. 법령을 위반한 정보주체에 대한 조사 또는 처벌 등 제재와 관련된 업무를 수행하기 위하여 공동이용이 불가피한 경우. 4. 그 밖에 법령에서 정하는 업무를 수행함에 있어서 정보주체의 사전 동의를 받는 것이 그 업무 또는 정보의 성질에 비추어 현저히 부적합하다고 인정되는 경우로서 대통령령으로 정하는 경우.

또 다른 연구 목적으로 사용되는 경우, 이 동의는 유효하지 않게 된다. 그러므로 현행 법률에서 언급하지 않은 동의의 유효기간, 재동의, 사후 동의는 정보주체의 자기결정권과 관련되어 발생할 수 있는 문제이다.

의생명과학연구를 하는 연구자들이 근거로 하는 법률은 '생명윤리 및 안전에 관한 법률'이다. 동 법 제16조에서는 인간대상 연구의 연구대상자들에게 서면 동의를 받기 전에 충분히 설명하여야 한다고 규정함으로써 '충분한 설명에 의한 동의(informed consent)'를 요청하고 있다. 즉 민감한 정보의 취급에서 발생할 수 있는 피해에 대하여 인체유래물 기증자를 보호하는 것이다.[122]

충분한 설명에 의한 사전 동의는 자신의 질병에 대한 치료방법, 의학적 연구 대상여부, 장기이식 여부 등에 관하여 충분한 설명을 들은 후에 이에 관한 동의 여부를 결정하는 것[123]이라고 할 수 있다. 밀러(Leslie J. Miller)에 의하면, '치료를 하기 전에 환자가 치료를 받을 것인지의 여부를 지식과 정보에 근거하여 선택할 수 있도록 치료절차를 환자에게 설명하고 그 치료에 내재되거나 수반되어 있는 실제적인 위협을 알리는 것'이라고 정의된다.[124] 따라서 인체에 대한 침습 행위에 대한 '충분한 설명에 근거한 동의' 방식과 연구 대상자들에게 요청되는 동의는 구별할 필요가 있다.[125] 왜냐하면 이와 같은 동의 방식의 목적과 개인정보자기결정권을 행사함으로써 정보주체가 얻을 수 있는 이익이 동일한지 살펴보는

122) Eleni Zika, et al., 2010, "Biobanks in Europe: prospects for harmonisation and networking. Institute for Prospective and Technological Studies", Joint Research Centre, European Commission, Brussels, Belgium: p. 115-129.

123) 보건의료기본법 제12조.

124) Leslie J. Miller, 1980, "Informed consent", JAMA, 244(18): pp. 2100-2103.

125) Ezelkiel J. Emmanuel, et al. 2003. Ethical and Regulatory Aspects of Clinical Research: Readings and Comments. Baltimore: The Johns Hopkins Univ. Press. pp. 189-224; informed consent에 대한 논의에서 강조되는 부분은 주어진 설명이나 정보가 동의의 내용과 관련된 부분을 모두 포괄하는지, 그리고 동의를 수행하는 사람이 그러한 설명이나 정보를 충분히 이해하고 자발적으로 동의하는지의 여부이다.

일이 중요하기 때문이다.[126] 요지는 환자와 의사와의 치료과정 속에서 여러 치료 대안들 중 하나를 선택하는 일련의 과정으로서의 동의와 자신의 정보를 활용해도 되는지를 결정하는 것과 같은 맥락의 동의인지 따져볼 필요가 있다.

자신의 개인정보처리가 법률에 의해 허용되었다고 해도 어떤 정보가 어떤 목적을 위하여 필요한지 명확하게 정보주체가 인식할 수 없다면 규범명확성의 원칙에 위배된다고 할 수 있다. 이는 동의를 받기 위해 제공되는 정보가 미래의 연구를 위한 것이므로 의사결정을 할 수 있을 만큼 이해가 쉽지 않을 뿐만 아니라 연구결과의 확실성이 충분하지 않을 수 있기 때문에 더욱 문제가 된다. 즉 아직 목표가 정해지지 않은 미래의 연구에 대한 위험과 혜택에 대한 정보를 듣고 동의하는 것이 매우 어렵다면, 이는 동의라고 말할 수 없다.[127]

동의의 절차도 중요하다. '생명윤리 및 안전에 관한 법률'에 근거한 동의 개념을 적용하면, 연구대상자에게 개인정보의 수집과 이용에 대한 적법한 절차로서의 관심의 초점은 동의를 받았다는 사실에만 놓이게 된다. 이러한 법률 적용방식은 개인정보자기결정권이 개인정보의 노출을 억제하는 데만 중점이 있는 것이 아니라 그 흐름을 적극적으로 통제하는 측면도 있다는 것을 간과한 태도라고 할 수 있을 것이다.

정보주체 입장에서는 자신이 직접 관련이 없는 연구에 대해 설명을 듣고 자발적으로 동의를 하는 것을 결정하는 것은 쉽지 않다.[128] 또한 비록 연구에 사용됨에 동의하고, 그 동의의 법적 성질이 조건 없는 양도라고 한다고 해도 그

126) 이상욱・조은희. 2011, "바이오뱅크의 바람직한 운영을 위한 공론화의 필요성", 생명윤리 12(1): 33-52면.

127) Henry T. Greely, 1999, "Breaking the stalemate: a prospective regulatory framework for unforeseen research uses of human tissue samples and health information", Wake Forest Law Review 34(3): pp. 737-766.

128) National Bioethics Advisory Commission, 2001, "Ethical and policy issues in research involving human participants", Volume I Report and Recommendations of the National Bioethics Advisory Commission, Bethesda: pp. 97-108.

폐기[129] 여부를 사전 동의 시 기증자의 의사만으로 결정할 수 있는가, 기증자가 어느 때 폐기를 요구할 수 있는가에 대한 규정도 마련되어야 한다. 이 문제는 인체유래물이 한 기관에서 다른 기관으로 이전하는 경우, 재 동의를 받을 수도 없는 경우에 더욱 구체화되어 나타날 수 있다. 즉 수집 당시에 이루어진 동의가 명시된 목적의 범위 안에서 그 정보의 보유자나 이용자에 대해서만 효력을 미치기 때문에 인체 유래물을 획득할 당시의 최초의 연구 목적이 아닌 다른 연구에 사용되는 경우에는 정보주체의 권리가 이차 활용에 미치지 않는다.

또한 바이오뱅크에 자신의 검체를 공여하지 않은 개인도 유전적으로 자신과 연관된 가족이나 유사한 질병을 앓고 있는 사람 등의 참여로 인해 간접적으로 자신과 관련된 정보가 포함될 수 있다. 그리고 인체유래물이 다른 연구에 사용될 수 있음을 고지 받지 못한 경우 자기와 관련된 정보들 가운데 어떤 것이 특정한 목적에 활용되는지 알 수 없다.

4.3.2 이차 활용을 위한 처리절차상의 쟁점

공공기관에서 수집된 생체·의료정보는 대규모의 데이터베이스를 통하여 의생명과학연구를 위하여 이차 활용된다. 생체·의료정보를 이차 활용하는 의생명과학연구는 궁극적으로 특정인을 분간하여 의료적인 혜택을 주기 위한 것이다.[130] 이러한 경우 가명화는 재식별을 지원할 수 있는 장점이 있다. 하지만 가명화는 개인의 신원을 보호하기 위해 별도의 가명의 식별자(pseudo identifier, 혹은 중개자)를 가진 코딩 시스템을 포함해야 한다(그림 10).

---

129) 생명윤리 및 안전에 관한 법률 28조 참조.

130) Anne Cambon-Thomsen, 2004. “The Social and Cultural Issues of Post-Genomic Human Biobanks” Nature Reviews Genetics 5: pp. 866-873.

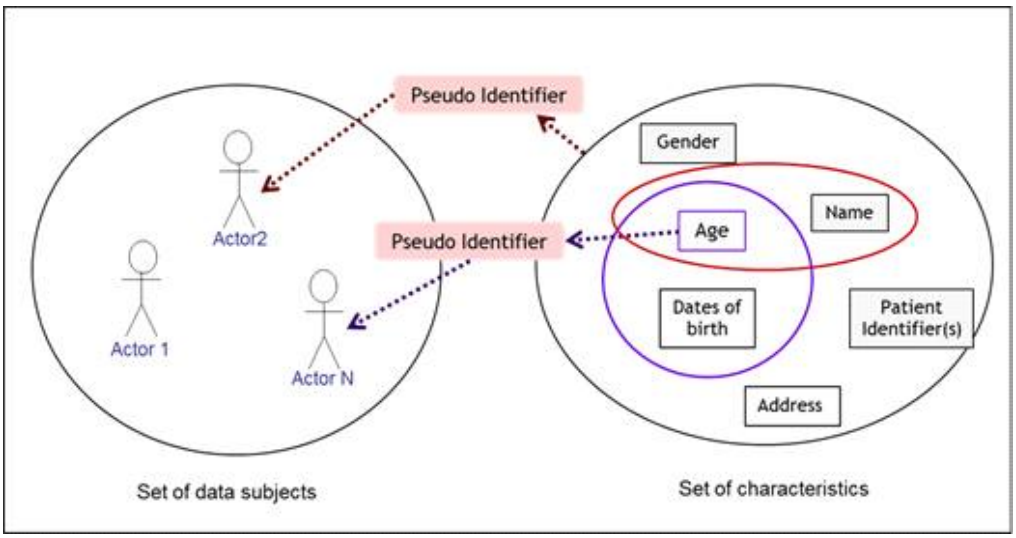

그림 10. 식별정보세트와 가명화 세트 (출처: ISO/IEC TS 25237)

이 가명의 식별자는 연구과정에서 실재 개인을 식별할 필요가 발생하는 경우, 생체정보 주체가 사망하는 경우, 생체정보가 도난당하는 경우 등을 대비하여 필요하다. 대부분 가명으로 사용되는 도메인이 다른 도메인과 어떻게 연결되는지 시나리오를 가지고 있다. 경우에 따라서는 권한을 가진 사람이 가명정보를 보관하고 있다가 필요한 때만 정보주체와 연결하여 식별하기도 한다. 따라서 이를 관리하는 사람의 역할은 매우 중요하다고 하겠다. 중간에서 가명과 실명을 연결하는 가명의 식별자를 누가 가지고 있는가가 쟁점이 될 수 있다.

'생명윤리 및 안전에 관한 법률'에 근거한 지침에서는 인체유래물 은행의 기관위원회 위원장, 인체유래물 획득기관의 보안책임자, 인체유래물 획득기관의 기관장들이 가명의 식별자를 관리할 수 있다고 명시되어 있다. 이런 경우 이차 활용을 하는 공통의 정보에 대하여 각각 다른 가명의 식별자를 각 공공기관이 별도로 보유하는 결과가 되어 정보주체가 열람, 정정 청구권을 행사하려면 적지 않은 시간과 비용이 소요 될 것이다.

개인식별성(identifiability)은 이차 활용에 있어 매우 중요한 의미를 가진다. 왜냐하면, 이차활용은 정보의 조합이다. 그래서 이러한 조합을 통해서 그 자체로 정보주체를 식별할 수 없는 정보라고 하더라도 동일성을 식별할 수 있는 정보(personally identifiable information)가 될 수 있다. 그렇게 되면 연구자 입장에서는 '개인정보보호법'에서 정의하는 '개인정보'[131]로 환원되어 연구진행과정에서 위법이 되는 것이다. 그리고 정보주체의 입장에서는 동의 면제를 승인 받을 수 있는 조건이 익명화였으므로 여기서 얻을 수 있었던 개인정보보호의 보호이익을 누릴 수 없게 된다.

익명화와 관련해서는 인체유래물은행 운영지침이 있다.[132] 동 지침에는 개인식별정보 중에서 암호화 대상을 명시하고 있다(표 5). 여기서 익명화 대상정보는 직접적 개인식별정보(Direct Identifier)이다.[133] 하지만 다른 정보들과의 결합을 통해 개인식별이 가능한 '간접적 개인식별정보(Indirect Identifier)'[134]로서 '잠재적 개인식별정보'에 대해서는 무엇을 암호화해야 하는지 분명치 않다. 잠재적 개인식별정보가 무엇을 지칭하는지는 알 수 없기 때문이다. 또한 잠재적 개인식별정보는 그 자체로는 개인식별정보가 아니므로 기관생명윤리위원회가 결정할 수 있는 대상이다. 그러나 개인정보보호법상 개인정보의 개념에는 개인의 동일성이 식별된 정보(personally identified information)뿐 아니라 동일성을 식별할 수 있는 정보(personally identifiable information)까지 포함된다. 즉 간접적 식별정보도 개인정보다.

---

131) 개인정보보호법 제2조1항 ; '개인정보'란 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상을 통하여 개인을 알아 볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

132) http://www.irb.or.kr/Home/html/menu08/PersonalInfoAndAnony.aspx

133) 인체유래물은행 관련 지침
http://www.irb.or.kr/Home/html/menu08/PersonalInfoAndAnony.aspx

134) 인체유래물은행 관련 지침에 명시된 간접적 개인식별 정보로서는 해당 개인의 친척, 고용주, 또는 가족의 성명, 특별하고 고유한 신원 확인적 특징, 희귀병이나 희귀 치료 또는 장애, 지역 거주민수가 작은 지역의 우편번호, 희귀한 직업이나 근무 장소 등이 명시되어 있다.

표 5. 인체유래물은행 관련 암호화 대상 개인정보

1	이름
2	생년월일(연령 계산 등을 위해 생년 월까지 기록하는 것은 해당하지 않는다. 단, 이때에는 이름, 주소 등의 추가 개인식별정보가 없어야 한다.)
3	사진
4	주소
5	주민등록번호
6	운전면허증번호
7	은행 계좌번호
8	전자메일주소
9	URLs(연구대상자의 식별 가능한 경우)
10	IP 번호(연구대상자의 식별 가능한 경우)
11	전화번호(연구대상자의 식별 가능한 경우)
12	팩스번호(연구대상자의 식별 가능한 경우)
13	의무기록번호 또는 환자등록번호
14	각종 자격증번호 및 학번 등
15	차량번호 (및 차량고유번호)
16	기타 식별 가능한 기호(잠재적 개인식별정보)

인체유래물은행 관련 지침에 대한 법효력의 문제와 생명윤리안전에 관한 법률과 개인정보보호법의 정합성을 따져야 할 것이다. 익명화 효과의 핵심은 추가 동의 획득 절차를 생략할 수 있다는 것이다. 하지만 실제로 바이오뱅크나 인체유래물질에는 같은 종류의 질병, 치료 방법 및 기증자를 식별 가능케 하는 모든 정보(personally identifiable information)가 함께 저장[135]되기 때문에 완벽한 익명화에는 한계가 있다.

익명화방법에 대해서도 쟁점이 있을 수 있다. 익명화 방법은 두 가지로 제시되며, 기관위원회 심의를 거쳐 한 가지를 선택할 수 있다. 그 중에 하나가 암호화인데,

135) Bernice S. Elger and Arthur L. Caplan, 2006, “Consent and anonymization in research involving biobanks: differing terms and norms present serious barriers to an international framework” EMBO reports no. 7(7): p. 661.

암호화란 즉각 판독 불가능한 코드화로 정의하고 있다. 이 방법이 모두 데이터 주체와의 연결을 제거하고 데이터 주체에 관한 특성의 특정 집합 사이의 연관을 끊어내는 가명화(Pseudonymization)[136]를 지칭하는지 그 방법론을 확인할 필요가 있다. 분명치 않은 점은 본 지침에서 제시하는 암호화 방법은 국가정보원에서 정하는 암호화 알고리즘에 준하도록 되어 있기 때문에 학술연구를 위한 목적과는 상이할 수 있다.

또 다른 문제점은 다른 조항에서 권고하는 익명화방법은 보안책임자가 암호화하는 경우와 인체유래물을 획득한 기관에서 암호화 하는 경우로 세분하고 있다. 그리고 복원이 필요한 경우 인체유래물은행의 기관위원회가 먼저 복원에 대한 결정을 승인하고 인체유래물을 획득한 기관에서 책임자들의 인증키를 통해 정보에 접근하도록 되어 있다. 이 조항은 복원할 수 있는 익명화를 전제하고 있다. 그렇다면, 암호화라는 용어보다는 익명화, 익명화라는 용어보다는 가명화(Pseudonymization)라는 용어를 사용할 때, 더 명확하고 구체적인 기술을 적용할 수 있을 것이다.

4.3.3 이차 활용을 위한 심의절차상의 쟁점

‘생명윤리 및 안전에 관한 법률’에서는 정보주체가 권리 행사를 할 수 없는 경우 기관생명윤리위원회[137]가 승인한다.[138] 연구대상자등으로부터 적법한 절차에

136) ISO/TS 25237, OID value set 1.0.25237.1: Pseudonymization is “a particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms.”

137) 제10조(기관생명윤리위원회의 설치 및 기능); ① 생명윤리 및 안전을 확보하기 위하여 다음 각 호의 기관은 기관생명윤리위원회(이하 "기관위원회"라 한다)를 설치하여야 한다.; ③ 기관위원회는 다음 각 호의 업무를 수행한다. 나. 연구대상자등으로부터 적법한 절차에 따라 동의를 받았는지 여부,; 라. 연구대상자등의 개인정보 보호 대책.

따라 동의를 받았는지 그 여부를 심의한다.[139] 하지만 이때의 기관생명윤리위원회는 연구자가 소속된 기관이므로 이차 활용에 쓰이는 생체·의료정보들을 안전하게 확보하는 것과는 별개이다.

'생명윤리 및 안전에 관한 법률'을 근거로 한 국가생명윤리심의위원회는 인간대상 연구의 심의 면제에 관한 사항을 심의한다. 그런데 가장 최근에 개최되었던 회의는 지난 2012년 5월 4일에 있었다. 제3기 위원회 구성 후 처음 개최되는 회의였는데, 부위원장 선출 등 위원회 운영 관련 사항 2건과 '생명윤리 및 안전에 관한 법률' 전부 개정에 따른 하위법령 심의[140] 등 총 3건의 안건을 심의하였다.[141] 우리나라는 과학기술부의 생명공학백서(2005년)에서 "생명공학은 생명체를 다루는 학문이기 때문에 국민에게 생명공학을 알리고 국민의 의견을 수렴하는 절차가 필요하다"고 정책방향은 밝히고 있지만, 세부적인 실행방안은 드러나지 않고 있다.[142]

---

138) 생명윤리 및 안전에 관한 법률, 제 16조 제3항; 제1항에도 불구하고 다음 각 호의 요건을 모두 갖춘 경우에는 기관위원회의 승인을 받아 연구대상자의 서면동의를 면제할 수 있다. 이 경우 제2항에 따른 대리인의 서면동의는 면제하지 아니한다. 1. 연구대상자의 동의를 받는 것이 연구 진행과정에서 현실적으로 불가능하거나 연구의 타당성에 심각한 영향을 미친다고 판단되는 경우. 2. 연구대상자의 동의 거부를 추정할 만한 사유가 없고, 동의를 면제하여도 연구대상자에게 미치는 위험이 극히 낮은 경우.

139) 제18조, 제38조, 제43조; 연구를 위해서 반드시 개별 동의를 받거나 또는 익명화 처리를 하여 기관위원회의 심의를 받아야 함. 연구란 '인간대상연구',; 사람을 대상으로 물리적으로 개입하는 연구, 설문조사, 행동관찰 등으로 자료를 얻는 연구, 개인을 식별할 수 있는 정보를 이용하는 연구와 '인체유래물연구'이다.

140) 생명윤리 및 안전에 관한 법률 제7조 2.공용기관생명윤리위원회의 업무에 관한 사항 (법 제12조제1항 제3호) 3. 인간대상연구의 심의 면제에 관한 사항 (법 제15조제2항) 4. 기록·보관 및 정보공개에 관한 사항 (법 제19조제3항) 5. 잔여배아를 이용할 수 있는 연구에 관한 사항 (법 제29조제1항 제3호) 6. 체세포복제배아 등의 연구 등에 관한 사항 (법 제31조제2항) 7. 배아줄기세포주를 이용할 수 있는 연구에 관한 사항 (법 제35조제1항제3호) 8. 인체유래물연구의 심의 면제에 관한 사항 (법 제36조제2항) 9. 유전자검사의 제한에 관한 사항 (법 제50조제1항).

141) 보건복지부 보도자료, 2012. 5. 4. 생명윤리안전과.

142) 이인영, 2006, "유네스코 '생명윤리와 인권보편선언'의 권고사항과 국내 실천을 위한 제언",

이 밖에 일반적인 조정절차의 한 종류로서 개인정보 분쟁조정위원회가 있다.[143] 정보주체의 개인정보와 관련한 당사자 간의 분쟁사건을 접수하여 합리적이고 원만하게 조정하여 해결하는 업무를 담당하는 준사법적 기구이다. '개인정보 보호법' 시행 이후 주요 분쟁사례는 기술적·관리적 조치 미비와 동의 없이 개인정보를 수집목적 이외의 목적으로 사용한 프라이버시 침해 사례였다.[144] 원래 조정은 법원에서 했지만 최근에는 분쟁조정위원회가 각 전문분야의 조정을 하고 조정이 성립된 경우에는 법원에서 한 것처럼 공적 효력을 부여한다. 이러한 분쟁조정의 효력이 실제로 이차 활용대상 정보주체의 열람, 정정, 삭제의 권리 보호를 위해서도 발생되게 하려면, 공공기관 간 이차 활용정보의 흐름을 투명하게 할 필요가 있다.

4.3.4 생체·의료정보 수집절차상의 쟁점

의료기기의 발전은 병원 밖에서 생체·의료정보가 자동으로 수집될 수 있는 기회를 제공하고, 이를 광범위하게 사용할 수 있도록 저장하기도 한다. 하지만 의료기기의 성능은 시간이 지남에 따라 혹은 플랫폼에 따라 그 결과 값이 실제 값과 차이가 날 수 있다. 그래서 민감정보를 수집할 수 있는 장치 및 의료기기의 고유한 주요 문제로서 프라이버시를 고려하고 있다. 미국의 경우 동맥경화 환자에게 쓰이는 동맥 스턴트(Stenting Emboli)의 승인을 지원하기 위해 다양한 수준의 부작용 평가를 하였다. 그리고 신경 내에서의 스턴트 볼륨과 위치 등에 대한 모니터링을 실시한 후에 임상안전성을 인정하였다.[145]

과학기술법연구 제12권 제1호: 9-37면.

143) 2011년, 개인정보보호법 제 40조에 의거하여 설치되었다.

144) 본인의 동의 없이 개인정보를 수집하고 이를 제3자에게 노출시킨 의료기관에 대한 제도개선요구(2012); 이용자의 개인정보를 파기하지 않고 광고문자 등을 발송한 여행 전문 업체에 대한 손해배상요구(2011).

의료기기는 의복형이나 신체 부착형으로 발전하고, 생체이식형 기기로 그리고 궁극의 방향은 생체 내장형기기로 발전할 것이다. 몸 안에 내장된 기기를 통하여 생체 내의 다양한 활동을 모니터링할 수 있는 날을 전망하는 것은 어렵지 않다. 생체에 내장된 센서가 혈관 내의 암세포를 발견하고 이 사실을 스마트 폰 앱을 통해서 실시간 진단 할 수 있는 가능성도 열려 있다. 의료인이 직접 특정한 목적을 가지고 수집하지 않아도 민감정보는 수집되고, 알 수 없는 이용자에게 전송되거나 저장 될 수 있다.

의료기기를 통하여 민감정보가 수집·저장·전송된다면, 이렇게 얻어지는 정보를 위한 정보 저장소(레지스트리)의 모양이나 디자인도 이를 감안해 맞추어져야 한다. 예를 들면, 장치의 수명과 샘플의 크기까지 고려하여야 할 것이고, 이차 활용을 염두에 둔 다양한 연구 설계에 따라 요구되는 데이터의 구성요소를 식별해야 할 것이다. 또 전송하기 전에 정보의 오류나 유출을 감지할 수 있는 적절한 기술적 초치가 내장되어야 할 것이다.

무엇보다 어떤 목적으로 다시 활용할 것인가를 알 수 없다면, 이차 활용하기 전에 원치 않은 사람의 손에 흘러들어가거나 정보 오류가 발생하지 않도록 해야 할 것이다. 즉 인체유래물의 종류, 사용자 인터페이스, 이미지, 음성 등의 캡처기술, 전자기적 간섭 등을 고려하여 의료기기를 만들 때부터 프라이버시 보호를 위한 장치를 마련해야 한다. 즉 프라이버시 보호는 정보주체에게서 분리되는 순간부터 이루어져야 한다.

---

145) Registries for Evaluating Patient Outcomes: A User's Guide, Third Edition 2014, "The Carotid Artery Stenting with Emboli Protection Surveillance Post-Marketing Study.", AHRQ; Case Example 58. Designing a registry to study the effectiveness of a device training program for providers.

4.4 생체·의료정보 이차 활용과 보호의 균형

공공정보 중에서 일반적인 개인정보와는 구별되는 민감정보에 해당하는 생체·의료정보의 이차 활용의 법적 근거와 문제점을 고찰한 결과, 일반적 개인정보와 그 보호기준을 달리해야 함을 알 수 있었다. 그 이유는 생체·의료정보가 개인의 사회적·인격적 사안과 관련되어 있기 때문이었다. 이로 말미암아 이차 활용하는데 더 강력한 제한요건이 필요하였다. 그럼에도 불구하고 생체·의료 정보는 공익목적의 연구를 위한 경우에는 동의가 면제되어 이차 활용이 가능하다. 그러나 여러 기관의 공공정보가 함께 이차 활용되는 경우가 대부분이므로 동의의 유효범위, 동의의 유효기간, 재동의, 사후 동의 등 현행법의 적용 범위 밖에서 발생하는 문제를 해결하기 위한 방안이 필요하다.

의생명과학연구대상자의 사전 서면동의는 기관위원회의 승인으로 면제될 수 있었다.[146] 하지만 엄밀히 말하면, 의생명과학연구의 주된 목적의 공개를 통하여 이차 활용을 장려하는 정부와 공공기관의 정당성을 추정할 수 있지만, 그 공익성을 판단하는 근거가 필요하다. 이차 활용은 여러 공공기관의 정보를 함께 이용하는 것이 대부분이므로 공공정보 등록 제도를 운영할 수 있는 위원회가 있어 이차 활용 대상 정보를 여기에 등록하고, 위원회는 그 내용을 승인할 수 있어야 한다. 우리나라에서는「공공데이터제공전략위원회」[147]가 그러한 역할을 할 수 있을 것이다.

이차 활용은 해당 정보를 가지고 있는 소수의 관련자들만으로 이루어지지 않는다. 생체·의료정보가 모아져서 이차 활용될 수 있도록 하기 위해서는 이차 활용의 결과로 인해 새롭게 창출되는 가치에 기존의 특정한 정치적·제도적

146) 생명윤리 및 안전에 관한법률 제16조

147) 공공데이터의 제공 및 이용 활성화에 관한 법률 제5조, 제6조.

이해관계를 가지고 있는 관련 공공기관까지도 편입시킬 수 있어야 한다. 이를 수행하는 새로운 제도가 필요한데, 동일한 목적의 이차 활용에 대하여 공통으로 제공되는 정보를 가진 공공기관 간 구속력이 있는 규칙을 근거로 함이 바람직하다.

한편, 익명성의 보장은 기술적용을 위한 절차 및 방법상의 문제도 환기시킨다. 이차 활용되는 생체·의료정보는 여러 공공기관의 보안책임자가 암호화하거나 인체유래물을 획득한 기관에서 암호화하는 것으로 세분하고 있는데, 이차활용 목적을 분명히 정하고 그 목적에 따른 익명화 방법을 동일하게 적용할 필요가 있다. 익명성의 확보는 기술적 조치만으로는 한계가 있기 때문에 익명화 방법, 익명화 처리과정, 익명화 정보의 복원 등과 관련된 사항을 확인하는 전문가의 개입이 바람직하다.

이차 활용을 위한 정보를 여러 기관에 동시에 요청하는 경우 이 판단의 과정을 어느 한 기관 내지는 한 연구자 개인에게 맡기는 것 보다는 국가 기관이 이를 대신해야 한다.「공공데이터 활용지원센터」[148]가 이 역할을 담당할 수 있을 것이다. 또한 생체의료정보의 수집이 여러 기관과 다양한 기기를 통해서 이루어지는 점을 감안하여 익명화된 정보를 수집하고 링크 후에도 오류를 방지할 수 있는 기술적인 기능과 데이터의 흐름을 모니터링하는 시스템을 설계하고 지원하는 역할도 해야 할 것이다. 공동심의제도도 필요하다. 우리나라에서는 그 법적 지위를 같이하는 개인정보보호위원회와 국가생명윤리심의위원회가 이차 활용되는 대상정보에 대하여 함께 심의하는 방안을 고려해 볼 만 하다. 제도 수행 방식은 연구를 시작하기 전부터 연구결과의 활용까지를 두루 파악할 수 있는 방식이 바람직할 것으로 본다. 이를 종합하면 그림 11과 같이 도식화할 수 있다.

148) 공공데이터의 제공 및 이용 활성화에 관한 법률 제13조.; 공공데이터 활용지원센터의 핵심 기능: 1.공공데이터 정책 제도기반 확립 2. 공공데이터 개방 관리체계 정비 3. 공공데이터 제공 및 이용 인프라 확충 4.공공데이터 기반의 창업지원 및 생태계 조성.

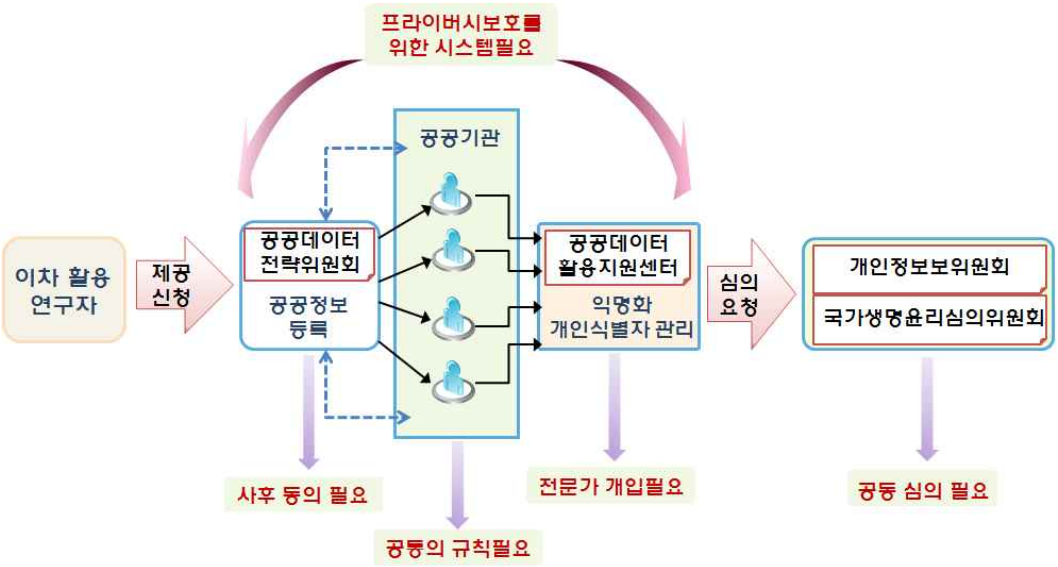

그림 11. 이차 활용을 위한 생체·의료정보 요청-제공 체계

요약하면, 이차 활용을 위한 생체·의료정보의 요청과 제공체계를 갖추기 위해서는 수집단계부터 익명화된 정보를 수집하고, 이차 활용 후에라도 정보주체의 개입이 가능한 사후동의 방식의 도입과, 익명화 및 복원화의 문제를 판단하는 전문가의 개입, 그리고 포괄적인 규제가 가능한 공공기관 간 공동규칙이 필요할 것이다. 그리고 개인정보보호와 공익성을 함께 추구하는 위원회의 역할을 개선하는 방안을 함께 고려해야 한다. 정부의 역할은 균형의 원리에 대한 유기적 일관성이 제자리를 찾아가는 것으로서, 다수에 포함되어 있는 사람들의 개인적 권리를 지키며, 동시에 개인의 권리를 무시하는 것을 정당화하는 것으로 볼 수 없는 공익을 구별해 줄 수 있을 것이다.

이차 활용과 관련해서는 오히려 비 식별정보였으나 다른 정보와 결합됨으로써 결과적으로 식별되는 개인정보가 이슈가 된다. 이점은 동의의 여부와 다른 법률의 근거가 존재하는 것과는 별개의 문제로 개인정보자기결정권을 통하여 보장되었던 익명성이 환원된다는 새로운 국면이 발생하는 것이다. 따라서 정보를 수집하는

단계에서부터 부정오류가 생기지 않도록 하는 시스템이 필요하며 재식별이 될 가능성을 염두에 두고 다시 비 식별조치를 취하거나 재 동의를 구하는 방법을 고려해야만 한다. 하지만 현행법은 재 동의나 추가동의는 허용하지 않고 있다. 또한 공공기관의 정보공유는 동의면제를 통해서 이루어지고 있다. 다만 민감정보를 별도로 취급하여 그 수집 및 처리를 원칙적으로 제한하고 있는데, 이 경우에는 오히려 공익의 개념을 간과하는 부분이 없지 않다.

다음 장에서는 외국 법률 및 국제기구의 가이드라인의 고찰을 통하여 생체·의료정보를 활용하는 공익목적들을 살펴보고, 동시에 프라이버시 보호를 위한 방법들을 도출하고자 한다.

제5장 생체·의료정보 관련 외국 법제도 비교분석

민감정보에 해당하는 생체·의료정보를 보호하는 우리나라의 법률에는 일반법으로서 '개인정보보호법'이 있고 의과학연구 등 이차 활용의 근거가 되는 법으로서 '생명윤리 및 안전에 관한 법률'이 있다. 그리고 공공기관에서 민감정보를 제공할 때는 다른 특별 법률에 근거한다. 생체·의료정보의 경우 정보주체의 프라이버시도 보호해야 하지만 공익을 위한 이차 활용도 허용해야 하는 현실적인 요구에 직면한다.

본 장에서는 현행 법률체계에서 문제점에 대한 새로운 개선방안을 도출하고자 외국의 민감정보 보호 방안과 이차 활용 방안을 비교분석한다. 우선 국제기구의 다양한 원칙들이 어떻게 개별국가에 입법기준이 되었는지 살펴보고, 미국식과 유럽식의 입법체계를 비교분석한다. 유럽연합 회원국가 중에서 프랑스의 개인정보 보호 기구를 살펴보고, 규제적 요소와 기술적 요소를 함께 시스템 디자인에 적용한 캐나다의 사례를 고찰한다.

5.1 생체·의료정보 보호를 위한 외국 법제도 비교분석

역사적 배경과 정보기술 수준에 따라 정보프라이버시를 이해하는 관점은 다르며 특히 미국과 유럽은 현저한 차이를 보인다.[149] 외국에서는 개별특별법 방식(sectoral model)의 미국식[150]과 일반법체계(omnibus model)의 유럽식[151]이 가장

149) Francesca Bignami, 2007. "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining." BCL Rev. No. 48: p. 609.

150) Daniel Solove, 2008. Understanding privacy, Cambridge MA, Harvard University Press: pp. 186-194.

151) 유럽에서는 1950년의 「인권 및 기본적 자유의 보호를 위한 유럽협약」(European Convention for the Protection of Human Rights and Fundamental Freedoms: ECHR)과 1981년의 유럽회의

현저한 차이를 드러내면서 각기 다른 방식으로 프라이버시 문제를 해결하고 있다.[152] 하지만 프라이버시는 양도하거나 양보할 수 없는 절대적인 가치가 아닌 상대적인 가치라는 것에는 이견이 없다.

이하에서는 국제기구의 다양한 원칙들이 어떻게 개별국가의 입법기준이 되었는지도 함께 살펴본다. 그리고 일반법으로서 공통된 개인정보보호법을 두면서도 분야별 입법에 의해 미비점을 보완하고 있는 유럽공동체[153]의 입법체계를 살펴본다. 이러한 유럽방식은 공공부문에만 개인정보보호법을 두고 민간부문에 대해서는 필요한 경우에만 분야별 입법을 하고 당사자들끼리 자율적인 규제로 대체하는 미국방식과 비교 가능할 것이다.

5.1.1 국제기구

경제개발협력기구(Organization for Economic Cooperation and Development, 이하 OECD)나 유럽평의회(Council of Europe, 이하 EC) 등 국제조직은 세계 각국의 입법에 영향을 미치는 개인정보보호를 위한 기본원칙이나 지침을 마련한다. 그 결과 각국의 개인정보보호에 관한 법제는 상당부분 닮아 가고 있다. 그러나 나라마다 정보통신 기술과 정보화 단계가 상이하여 개인정보보호에 관한 법을

협약 「개인정보의 자동처리와 관련된 개인의 보호를 위한 유럽회의 협약」(Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Euro, T.S. No.108: CoE 108)에 이어 유럽공동체가 1995년 「개인정보의 처리에 관한 개인의 보호와 개인정보의 자유이동을 위한 준칙」(Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data)을 채택하기에 이르렀다.

152) Robert Rocco Cottone, 2001, "A social constructivism model of ethical decision making in counseling." Journal of Counseling & Development no. 79 (1): pp. 39-45.

153) Richard Tutton, 2010, Biobanking, "Social, Political and Ethical Aspects, Encyclopedia of Life Sciences", Chichester, John Wiley & Sons: pp. 1-7.

비교분석하기 어려운 요소가 있다. 또 이러한 과학기술 환경이 반영된 사회적 여건과 문화의 차이로 인해 일률적으로 적용할 수 있는 비교 기준을 설정하는 데도 곤란을 겪는다. 그럼에도 불구하고 무역과 밀접한 관계가 있는 초국가 공동체에서는 일정한 기준을 충족하면서 서로 통일된 규칙이 필요하였다. 즉 각국 간의 무역에 있어서 개인정보의 수집과 이전이 수반되는 경우가 많았고 원활한 개인정보의 흐름이 뒷받침 되어야만 무역도 원활하게 될 수 있었다. 이러한 상황에서 각국의 개인정보보호법의 통일을 위한 국제적 논의가 활발히 진행이 되었다.

본 논문은 국제기구의 개인정보보호에 관한 규범들을 살펴봄으로써 공동의 목적을 위하여 정보를 가진 기관끼리 협력할 수 있는 방안을 모색해 보고자 한다.

5.1.1.1 유럽평의회의 개인정보보호협약

유럽평의회는 유럽통합에 있어 가장 오래된 조직체이다. 1950년 유럽평의회는 다자간 국제조약으로서 국가 안보를 위하여「유럽 인권 협약 (European Convention on Human Rights, 이하 ECHR)」을 도입하였다. 유럽인권협약은 기본권의 효력을 규정하고, 기본권보호를 위한 위원회와 법원을 설치하고 있다. 그리고 법원의 판례는 비례원칙을 근거로 한다.[154] 비례원칙의 형식적 구조는 3단계의 심사이다. 즉 첫째, 국가의 조치는 추구하는 목적의 달성에 적합한 것이어야 한다. 둘째, 그것은 필요한 최소한의 것이다. 즉 '가장 경미한 조치' 또는 '가장 최소한으로 침해적인 조치'가 요구된다는 것이다. 셋째, 협의의 비례성이다.

154) 유럽법원의 'Fedesa' 사건에 대한 판례, EuGHE 1990 I - 4023,; 당원의 확립된 판례에 따르면 비례원칙은 유럽공동체법의 일반원칙에 속한다. 비례원칙에 의하면 어떤 경제적 활동을 금지하는 조치는 그것이 당채 규제를 통해 추구되는 목적에 적합하고 필요한 것일 때에 한하여 적법하다. 수개의 적합한 조치들이 있을 때에는 그 중 침해적 효과가 가장 작은 것을 선택하여야 한다. 나아가 그 조치로 야기된 침해는 그것을 통해 추구되는 목적과 비례관계에 있어야 한다.

이는 일정한 공적 목적의 추구를 위한 조치가 그 목적과 비례관계에 있지 않은 손해를 초래하여서는 안 된다는 의미이다. 특히 이 세 번째 단계가 목적과 수단의 관계를 설명해 주고 있는데, 만일 효용보다 많은 손실을 초래할 때에는 그 조치는 중단되어야 한다는 것이다. 비례원칙은 공동체의 법제정과 행정결정을 통제하기 위한 원칙이라고 할 수 있다.[155]

5.1.1.2 경제협력개발기구 가이드라인

OECD에서도 공공정보의 상업적 활용에 대한 중요성을 역설하고,[156] 2008년에는 장관회의에서 주요 의제로 채택하여 각국의 노력을 강조하였다.[157] 그 중에서 「프라이버시보호와 개인데이터의 유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」은 국제적으로 원활한 정보유통의 기반을 만들기 위해서 국내법제의 조화를 목적으로 하고 있다. 따라서 가입국간의 무역과 경제협력 증진을 위하여 자유로운 정보유통과 합법적인 제한이 그 기본취지이다.[158] 이 가이드라인이 나오기 전 유럽과 미국은 개인정보를 둘러싸고 다소 긴장관계에 있었다. 즉 유럽의 입장에서는 정보의 흐름을 보장해야 한다는 미국의 주장을 시장에서의 주도권 유지를 위한 것으로 해석하였다. 반면, 미국의 입장에서는 유럽의 강한 개인정보보호 주장을 보호무역의 일환으로 해석하였다.

회원국이 지켜야하는 가이드라인은 개인정보보호의 일반적인 원리라 할 수

155) 폴크마르 괴츠, 1997, “유럽법의 일반원칙으로서 비례원칙과 신뢰보호원칙”, 서울대학교 법학 제 38권 3·4호: 31-43면.

156) OECD, 2006, A Workshop on Access to Public Sector Information and Content. http://www.oecd.org/sti/44384673.pdf.

157) OECD, 2008, A workshop on public sector information held to prepare the OECD Recommendation.

158) OECD 1980, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

있는 여덟 가지 원칙을 명확하게 제시하고 있다.[159] 여덟 가지 원칙은 다음과 같은 특징으로 요약할 수 있다. 첫째, 개인정보 해외로의 이전이 방해되지 않고 보장되도록 합리적이고 적절한 조치를 취하여야 한다.[160] 둘째, 상대국가가 이 가이드라인을 실질적으로 준수하지 않거나 국내법을 회피하기 위한 경우를 제외하고는 개인정보의 해외 간 이전을 제한하여서는 안 된다.[161] 셋째, 프라이버시와 개인의 자유의 보호라는 이름으로 개인정보의 해외 간 이전을 방해하는 법률, 정책, 집행을 피해야 한다.[162]

가이드라인의 형식으로 제시되는 원칙은 법적 구속력이 없는 권고안으로서 이를 받아들이는데 큰 부담이 없다. 이런 점은 EU의 준칙(directive)에 대해서도 마찬가지 입장인데, 유럽연합의 회원국들은 나라마다 상이한 현실적인 기술발전 상황을 적용하여 자국의 국내법을 만들 때, 그 토대가 되는 공통의 원칙으로서 EU 준칙을 활용하고 있다.[163]

---

159) 95/46/EC, 1995. Directive of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data: 수집제한의 원칙(Collection limitation principle), 정확성의 원칙(Data quality principle), 수집목적 명확화의 원칙(Purpose specification principle), 이용 제한의 원칙(Use limitation principle), 안전 확보의 원칙(Security Safeguards Principle), 공개의 원칙(Openness Principle), 개인 참여의 원칙(Individual Participation Principle), 책임의 원칙(Accountability Principle).

160) OECD Guideline 16; Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

161) OECD Guideline 17; A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

162) OECD Guideline 18; Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

5.1.1.3 아시아 태평양 경제협력체 개인정보의 안전한 이전을 위한 인증제도

APEC은 2003년부터 효과적인 개인정보보호의 중요성을 인식하고 개인정보 보호 방안을 구체적으로 모색하였다. 2004년에 아시아 태평양 지역의 21개 회원국 간의 개인정보의 안전한 이전을 위한 프레임워크를 채택하였다.[164] 이는 회원국가에게 구속력은 없지만 자발적인 약속에 근거한 개인정보보호의 기준을 개선하는 수단이 되었다.[165] 이 프레임워크의 목표는 아시아 태평양 지역 전반의 전자 상거래 촉진이다. 무엇보다 개인정보처리자의 내부 개인정보 보호규칙의 이행을 촉진시키는 것을 목적으로 한다. 그래서 해외 이전 시 개인정보의 보호에 관한 OECD 가이드라인의 핵심 가치와 일치한다.

2006년에는 자발적으로 해외이전을 위한 인증제도(Cross Border Privacy Rules, 이하CBPR)를 채택하였다.[166] CBPR의 원칙은 개인정보처리자의 책임에 대한 명확성, 제3자에 대한 구속력의 명확성, 개인정보 처리의 명확성, 개인정보 처리 근거에 대한 명확성, 개인정보처리에 대한 정보주체 고지에 대한 명확성으로 요약할 수 있다(표 6).[167]

---

163) 95/46/EC, 1995. Directive of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data.

164) 미국, 중국, 일본, 한국, 러시아, 오스트레일리아, 뉴질랜드, 페루, 인도네시아, 멕시코, 싱가포르, 태국, 베트남 등.

165) APEC, Privacy Framework, Nov. 2004, a meeting in Santiago, Chile.;: (i) preventing harm; (ii) notice; (iii) collection limitation; (iv) use of personal information; (v) choice; (vi) integrity; (vii) security safeguards; (viii) access and correction; and (ix) accountability.

166)APEC CROSS-BORDER PRIVACY RULES SYSTEM: pp. 3-19
http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx;

167) APEC Cross-border Privacy Enforcement Arrangement, 2004.

표 6. APEC CBPR의 원칙

개인정보관리자의 책임에 대한 명확성	정보관리자(controller)는 다음의 어느 하나 이상의 요건에 의하여 내부 개인정보 보호 규칙을 입증함으로써 개인정보처리자의 책임을 명확히 함. 또한 내부 개인정보 보호 규칙과 관련하여 교육을 실행하기 위한 절차를 만들어야 함.
제3자에 대한 구속력의 명확성	정보관리자는 기술적 안전성 및 관리적 조치 등을 충분히 보장할 수 있는 공공기관, 위탁처리자, 기타 서비스 제공자를 선정해야 함. 특히, 정보관리자는 위탁처리자(processor)를 지도하여야 함.
개인정보 처리의 명확성	정보주체의 동의를 위한 개인이 요청할 경우, 법률 당국이나 다른 법률적 도구 및 법률 효과의 선포 및 선언 등에 의한 서비스 또는 상품의 제공에 필요할 경우, 다른 호환 가능한 또는 관련된 (compatible or related) 목적으로 사용가능함.
개인정보처리 근거에 대한 명확성	개인정보처리자의 내부 개인정보 보호 규칙은 다음 내용의 임무를 포함해야 함. (1)개인정보는 정보주체로부터 고지에 기반을 둔 동의 등 처리에 대한 유효한 근거가 있을 때에만 처리될 수 있어야 함. (2) 개인 데이터는 적용되는 법률과 일관되게 처리되어져야 함.
개인정보처리에 대한 정보주체 고지에 대한 명확성	정보주체는 해당 개인정보의 수집, 이용, 공개에 관한 사후 동의 선택권을 제공받아야 함. 개인정보관리자는 개인 데이터가 어떻게 수집되고 있는지에 대하여 정보주체에게 고지하여야 함.

CBPR은 국내 법률로서의 효력은 없기 때문에 인증을 받는다고 할지라도 법적 요구사항을 준수하는 것으로 간주되지는 않는다. 인증체계는 다만 보충적 조치에 불과하므로 인증을 받은 기관은 여전히 자국의 법적 요구 사항을 계속해서 준수해야 한다.

CBPR의 내용에는 개인정보관리자가 정보주체로부터 동의를 받거나 혹은 제3자가 해당기관의 내부 개인정보 보호 규칙을 일관되게 준수할 것인가를 사전에 실사(due diligence)하기 위한 지시사항(instructions)이 포함되어 있다. 이 지시사항을 통해 의무이행에 필요한 기밀사항과 규칙을 지도해야 한다. 지시사항의 내용에는

정보주체의 동의뿐만 아니라, 개인의 요청, 법률 당국이나 다른 법률적 도구 및 법률 효과의 선포 및 선언 등이 포함되어 있다.[168] 특히 민감정보는 피해위협, 데이터의 민감도, 환경적 맥락의 가능성 및 심각성에 비례(proportional)하여 안전성이 확보되어야 한다.

5.1.2 유럽연합

5.1.2.1 유럽연합 준칙들

유럽연합(European Union)에는 두 가지 유형의 법률이 있다. 미국의 법률과 같은 규제(Regulation)와 각 회원국들이 자국에서 국내법으로 구현할 수 있는 일반적인 준칙(Directive)이 있다. 이 준칙은 회원국들에게 공통으로 구속력을 발휘하며, 국내법이나 국내규제가 도입되어 각국의 서로 다른 규제들이 서로 조화를 이루도록 한다.

1995년 2월 '개인정보의 처리에 관한 개인의 보호와 개인정보의 자유이동을 위한 준칙(Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data; 이하 EU 지침)'을 제정하였다[169]. 이 지침의 기본 취지는 정보의 자유로운 유통을 저해하는 장애요인을 없애고 동시에 회원국의 국내입법을 개인정보보호를 위하여

168) APEC, 2004, 프라이버시 프레임워크 제3장 제4원칙: pp. 16-17, 프로그램 자격요건: pp. 8-10.
http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

169) On February 20, 1995: the Council of Ministers adopted a Common Position with a View to Adopting Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

통일하는 것이다. EU 지침은 유럽공동체의 회원국이 각국의 입법을 위한 초안의 형태로서 1998년 10월 그 효력이 발생되었는데, 이 준칙에 따라 자율적으로 3년 내에 여섯 가지의 법률적 기본 원칙에 따라 국내입법을 해야 했다(표 7).

표 7. 유럽연합 준칙(Directive 95/46 EC)의 여섯 가지 기본원칙

고지 (Notice)	개인은 자신의 정보가 수집되는 것을 알 권리가 있다. 개인정보는 명시적이고 합법적인 목적을 위하여 수집되고, 목적에 맞지 않는 방식으로 처리 되서는 안 된다.
선택 (Choice)	개인은 자신의 개인정보의 수집에 반대할 권리가 있다.
이용 (Use)	개인은 자신의 개인정보가 어떻게 이용되는지 알고 그 이용을 제한할 수 있다. '정당한 처리'의 경우에만 이용되어야 한다.
보안 (Security)	개인은 자신의 개인정보를 보호하는 정도를 알 권리가 있다. 기관은 개인정보를 보호하기 위해 적절한 기술적, 조직적 조치를 취해야 하며, 위험에 대비한 적절한 조치여야 한다.
수정 (Correction)	개인은 자신의 개인정보를 정확한 것으로 수정할 권리가 있고, 기관은 부정확하거나 불완전한 정보를 수정하도록 관리해야한다.
법률적용 (Enforcement)	개인은 개인정보보호의 권리를 위하여 적절한 법적 구제요청을 할 수 있다.

하지만 이 준칙에서 적용하는 정보 이전에 대한 일반법의 예외적용조건을 주목할 필요가 있다. 그 내용은 첫째, 정보주체의 명확한 동의가 있을 때, 둘째, 정보주체와 관리자 또는 관리자와 제3자간의 계약에 의한 것일 때, 셋째, 중요한 공공이익 또는 법적 소송을 수행하거나 방어하기 위해 필요할 때, 넷째, 정보주체의 중요한 이익을 보호하기 위해 필요할 때 등이다. 즉 이 경우에는 민감정보를 처리할 수 있다. 정당한 목적을 위한 수집, 목적에 부합하는 처리, 목적과 수집 및 처리의 비례성, 정보의 최신성, 정보주체의 접근권 등의 원칙은 개인정보처리의

적법성과 관련된 것이며, 민감정보 처리 원칙이라고 할 수 있다.[170]

「개인 데이터 처리에 관한 유럽 협약(Council of Europe Convention on Personal Data Processing)」은 자동화된 개인정보 처리에 관한 협약[171]으로서 다른 국제협약과 마찬가지로 회원국에 법적 구속력이 있다.[172] 이 협약에는 인종, 정치적 의견, 종교, 건강, 성생활, 전과 등은 특별범주로 구분하여 적절한 보호책이 마련되지 않는 이상 자동처리 될 수 없다고 규정한다.[173]

의생명과학연구 목적의 의료정보는 익명으로 해야 하지만 익명성 보전이 과학연구 프로젝트 진행을 불가능하게 할 경우, 그리고 해당 프로젝트가 합법적인 목적으로 진행되는 경우에는 다음과 같은 조건에서 개인정보를 이용하여 프로젝트를 진행할 수 있다.[174]

(1) 정보주체가 하나 이상의 연구 목적에 대해 명확히 동의한 경우,

(2) 해당정보주체의 법적대리인 또는 법률이 정한 기관이나 개인 또는 단체가 정보

---

170) EU 지침 제 8조 : "인종적·정치적 의견, 종교적·사상적 신조, 노동조합의 가입, 건강 또는 성생활 등에 관한 민감한 개인데이터(sensitive personal data) 처리는 원칙적으로 금지"한다고 그 원칙을 밝히고 있다.

171) The Council of Europe's Data Protection Convention opened for signature on 28th of January 1981; Under this convention, the parties are required to take the necessary steps in their domestic legislation to apply the principles it lays down in order to ensure respect in their territory for the fundamental human rights of all individuals with regard to the processing of personal data.
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

172) Council of Europe, 1981, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. http://epic.org/privacy/intl/coeconvention/

173) Dudgeon v. United Kingdom, In a 1981 case 52: the European Court of Human Rights (ECHR) ruled that Northern Ireland's sodomy law violated Article 8 of the European Convention on Human Rights; Nov. 4, 1950. Convention for the Protection of Human Rights and Fundamental Freedoms, Article 8, 213 U. N. T. S. 221, 230.

174) Council of Europe Committee of ministers, Recommendation No. R(97)5. on The protection of Medical data.

주체의 의료 조건 또는 질병과 관련한 연구 프로젝트의 프레임워크에 동의를 한 경우,
(3) 중요한 공공 이익과 관련한 정해진 과학 연구 프로젝트의 목적을 위해 정보가 공개되는 것을 국내법이 정한 단체(들)이 승인한 경우.

5.1.2.2 BCR 제도

유럽연합의 프라이버시 감독조직인 제29조 실무 작업반(WP29)은 유럽집행위원회의 조정을 통해 모든 다자간 또는 양자 간 합의를 포괄할 수 있도록 데이터보호수준을 요구된 보호 수준만큼 높일 수 있도록 하였다. 그리고 EU 지침 제27조를 근거로 이 지침의 시행을 원활하게 하기 위한 행동강령(code of conduct)을 마련하도록 하였다.[175] 이 강령에는 EU의 개인정보보호원칙을 준수하겠다는 서약과 함께 정보주체를 위한 각종 권리구제수단이 명시되어있어야 한다.[176] 그리고 이를 실행하는 방법으로서[177] 회원국 간의 안전한 개인정보 유통을 위해 사전에 승인을 요하는 계약의 형태를 규정하였다. 이 수행 절차가 '보충성 원칙(Principle of Subsidiarity)'에 근거한 'Binding Corporate Rules(이하 BCR)' 제도이다.[178]

보충성의 원칙은 유럽연합의 다층적 구조에서 회원국가의 권한 분배와 행사에

175) Christopher Kuner, February 2005, "Using Binding Corporate Rules for International Data Transfers: The ICC Report", Electronic Banking Law and Commerce Report, Glasser Legal Works, Vol 9, No. 8: p. 3

176) Working Party document WP 108, "Working Document establishing a model checklist application for approval of Binding Corporate Rules", adopted on 14 April 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf

177) The Treaty on European Union §5.

178) Commission Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC (Text with EEA relevance) http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_en.htm

관한 기본 원칙이다.[179] 보충성의 원칙이 유럽연합에 공식적으로 도입된 것은 1992년 마스트리히트 조약이다.[180] 유럽연합의 회원국들이 자신들의 권한을 각기 주장할 경우, 권한의 충돌이 발생할 수 있는 여지가 있으므로 '하위 단위의 공동체에 의해 만족할 만하게 추구될 수 있는 기능의 수행은 상위 단위체가 담당해서는 안 되며, 하위체가 충분히 만족시킬 수 없는 기능의 수행에 있어서만 상위체의 도움을 받는 것'을 의미한다.[181] 이때 보충성이란 유럽공동체 회원국들이 변동이 있을 때 그 법적 대상이 되는 영토와 경계를 지속적으로 법에 반영하는 것이다. 즉 공동체의 행위가 권한 영역과 상대적 효율성이라는 적용기준에 따라 효과적으로 제한 될 수 있다.

이러한 맥락에서 BCR은 제 3국에의 정보 이전을 위한 안전조치로서 구속력 있는 규칙이라고 할 수 있다. 수행 방식은 기업 활동을 관할하는 회원국의 개인정보감독기관이 개인정보보호에 필요한 조치(safeguards)를 갖추었다고 승인(authorization)하면 여타 회원국 감독기관들도 이를 따라서 인정한다. 시행 초기에는 정보 이전의 안전장치로서 BCR을 활용하는 것에 대해 적절한 보호 수단으로 인정할 수 없다는 회원국이 있었다.[182] 그러나 오늘날에는 대부분 이를 인정하는 추세로 바뀌었다. 이제는 범 유럽 차원에서 BCR를 공통의 개인정보

---

179) EC Treaty 3B 참조: '공동체의 배타적 권한이 아닌 영역에서, 회원국들에 의해 충분한 성관가 나타나지 않는 경우에, 적절한 범위 내에서 공동체는 행동한다.'

180) Akos G. Toth, 1992, "The principle of subsidiarity in the Maastricht Treaty", Common Market Law Review no. 29: pp. 1079-1079.; The European Community law reflects this continued commitment to territorial and sectoral boundaries. Under 'subsidiarity,' the European Community may only act on matters that are not more properly within the boundaries of member-state competence.

181) Oreste Pollicino, 2008, :European Arrest Warrant and Constitutional Principles of the Member States: a Case Law-Based Outline in the Attempt to Strike the Right Balance between Interacting Legal Systems", German Law Journal Vol. 9 No. 10: pp. 1313-1355.

182) EU-US Workshop on Safe Harbor Framework Bridging Differences in Approaches to Data Protection, Washington, DC, December 7, 2005.

보호 절차로서 인정하도록 하고 있다.[183]

BCR은 표준계약서형태이다. 각 회원국의 개인정보처리 원칙을 존중하고 해당 국가의 관련법규를 준수할 것을 공동으로 서약하는 형태이다. 만약 유럽 공동체 이외의 제3국에 소재하는 기업그룹에 정보를 이전하는 경우에는 EU집행위원회가 채택한 BCR 조항을 따르면 된다.

계약당사자는 정보 전송자(data exporter)와 정보 수신자(data importer)이다. 계약 내용은 개인정보보호 규정을 준수하고, 정보주체가 계약서에 보장된 제3자의 수익권에 동의하는 것을 골자로 한다.[184] 제 3의 수익자(third party beneficiary)의 권리의 보장은 법적 권한이 있는 유럽위원회가 결정한다. 바로 이점이 BCR이 구속력이 있는 이유가 된다. 다시 말하면, 정보주체의 개인정보 침해 사안을 유럽연합의 보편적 이익으로 대변하고 공동체의 공동의 목표와 정책을 균형 있게 실행하며, 이를 위한 강력한 집행권이 있는 위원회의 심의가 제3의 수익자의 권리를 보장할 수 있도록 하는 절차가 된다.

2005년 EU집행위원회는 BCR을 중간 평가하고 조항을 추가하여 계약당사자로서 정보관리자 대 정보관리자(controller to controller),[185] 정보관리자 대 정보처리자(controller to processor)[186]를 인정하였다. 정보처리자는 정보 이전을 위한 개인정보 익명화를 담당한다. 정보관리자 외에 정보처리자가 계약의 당사자로 인정된 것은 그 만큼 정보화 기술이 낳은 문제점을 법률안에서 해결하고자하는 의지로 해석할 수 있다.

BCR을 준비하기 위해서는 아래와 같은 문서가 갖추어져야 한다.

---

183) Working Party 29 paper N.74, 3 June 2003 ; Working Party 29 paper N.107, 14 April 2005; Working Party 29 paper N.108, 14 April 2005.

184) Explanatory Document on the Processor Binding Corporate Rules, Adopted on 19 April 2013, ARTICLE 29 DATA PROTECTION WORKING PARTY: EU BCRs에 대한 설명 참조.

185) Commission Decision 2001/497/EC; Commission Decision 2004/915/EC.

186) Commission Decision 2002/16/EC.

(1) 해당 기관의 개인정보보호 방침(국민용/ 개인정보처리자용)

(2) 교육 프로그램 설명

(3) 내부 민원 처리 시스템에 대한 설명

(4) 정보처리를 위탁한 경우, 외부의 개인정보처리자와 맺은 표준 계약서

EU 지침은 BCR의 행동강령에 적시된 기준에 미치지 못할 경우 개인정보의 제3국으로의 이전을 금지하도록 하였다. 그리고 다음 경우에 해당할 때에만 민감정보의 처리가 가능하다고 되어 있다.[187]

(1) 법률이 허용하는 범위 내에서 정보주체가 자신의 민감정보 처리에 명시적으로 동의한 경우.

(2) 적절한 보호를 제공하는 회원국의 법률에 의해 승인 받은 범위 내에서 EU 근로계약법이 적용되는 분야에 대하여 통제자의 의무와 특정 권리를 수행하기 위한 목적 달성에 필요로 하는 경우.

(3) 정보주체 또는 해당 정보주체가 물리적 또는 법률적으로 동의를 표명하기 어려울 때 정보주체의 중대한 이익을 보호하기 위한 경우.

(4) 정치적, 철학적, 종교적 혹은 노동조합의 목적을 수행하는 재단, 사단 혹은 기타 비영리단체에게 적절하게 보장된 정당한 활동의 과정에서 수행되는 처리인 경우. 단, 해당 단체의 회원 또는 당해 단체의 목적과 관련한 정기적인 접촉을 가지는 사람에 관련된 처리에만 한하며, 정보주체의 동의가 없다면 제3자에게 공개되지 않을 것을 조건으로 함.

(5) 정보주체에 의해 명백히 공개되어진 민감정보와 관계되는 처리인 경우.

(6) 민감정보의 처리가 법적 권리행사(legal claim)의 개시, 이행, 방어를 위해 필요한 경우.

(7) 예방의학, 의학적 진단, 혹은 치료의 제공 또는 건강관리 서비스의 운영을 목적으로 하는 경우.

187) EU: 개인정보보호지침 95/46, 8조; WP154, 6장 참조.

(8) 국내법 또는 직업적 비밀유지의 의무가 있는 정부기관에 의해 제정된 법률 또는 규칙 하에서의 비밀유지 의무가 부여된 사람에 의하여 처리되는 경우.

EU 지침의 내용 중에서 가장 중요한 내용은 회원국으로 하여금 개인정보보호와 관련된 감독기관의 설치를 의무화하고 그 법률의 준수를 모니터링 하도록 한다는 점이다. 따라서 감독기관은 정부나 다른 기관으로부터 완전히 독립될 것이 요구되었고, 조사권, 개입권, 소송 수행권, 청문권 등의 권한과 책임을 부여하도록 하고 있다. 이러한 권한과 책임은 전통적으로 개인정보를 보호하는 정부기구들에게 요구되고 있다.[188]

아래에서 프랑스의 정보보호 감독기구를 고찰을 통하여 이러한 원칙들이 어떤 방향으로 발전되고 있는지 살펴본다.

5.1.3 프랑스

프랑스는 1974년 3월 정부가 가지고 있는 모든 고유한 개인 신원정보를 행정기관이 상호 연계하는 계획을 발표하였다. '사파리(SAFARI; système automatisé pour les fichiers administratifs et le répertoire des individus)'라고 알려진 이 시스템이 구축하려는 정보는 1970년대부터 통계청에 보관된 프랑스 전 국민의 사회보장번호다. 이 번호는 근본적으로는 1941년부터 프랑스 행정부가 만들기 시작한 것이다.[189] 사파리 계획이 발표되자 국민들은 즉각적으로 사생활과 개인의 자유가 크게 위협받을 가능성이 높다고 강력하게 반발하였다. 이를

188) Colin J. Bennett and Charles D. Raab, 2006, The Governance of Privacy - Policy Instrument in Global Perspective, Cambridge MA, MIT Press: pp. 95-120.

189) An article in 'Le Monde' 1974, with the headline "Safari, or the Hunt for Frenchmen" reported on a project called Safari, which involved a plan to link various government databases of personal information.

계기로 대통령 명령을 통하여 공공·민간부문을 통합한 감독기구를 설치하도록 하고, 개인정보처리시스템에 관하여 자문·감독·조사 등의 임무 수행을 맡겼다.

그 후, 공공기관의 시스템 설치에 대한 사전 허가제, 정보시스템 감독, 정보주체에게 본인의 정보에 대해 접근할 수 있는 권리 인정 등을 골자로 독립기관의 설립에 관한 법률안이 상정되었고, '정보처리·축적 및 자유에 관한 법률 1978. 1. 6 (Loi n°78-17 du 6 janvier 1978 relative al'informatique, aux fichiers et aux libertes, 이하 정보처리법)'이 제정되었다. 동 법은 정보처리의 결과로서 초래될 수 있는 기본적 인권, 사생활, 개인적 또는 공적 자유에 대한 침해를 방지함을 목적으로 하고 있다.[190] 정보처리법을 근거로 하여 '국가정보처리자유위원회(Commission Nationale de l'Informatique et des Libertés, 이하 CNIL)'가 설립되었다.[191]

프랑스는 정보처리시스템의 설치와 관련하여 공공부문과 민간부문이 그 규율을 달리하고 있다. 공공 부문은 미리 CNIL의 허가를 요하고 민간부문은 신고할 것을 요구한다.[192] 즉 국가·공공기관이나 지방자치단체 또는 공익사업을 하는 사법상 법인을 위하여 처리되는 개인에 관한정보는 원칙적으로 CNIL의 의견을 청취한 후에 정해진 법규에 따라 그 처리를 결정한다.

정보처리법에 의하면, 정보처리의 결과가 불이익이 되는 경우 그 정보와 이유를 알권리가 있고(Article §3; 공정하고 적법한 수집·처리), 개인에 관한 정보의

---

190)Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Article 1 En savoir plus sur cet article: L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

191) Publication au JORF du 7 janvier 1978, Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004, version consolidée au 24 janvier 2006 - version JO initiale.

192) EU의 e-Privacy Directive의 유출통지 요구사항에 대한 요구를 반영하여 Data Protection Act 34조 개정.

자동처리가 개인의 권리와 이익을 침해하지 않은지 정보주체는 자신의 정보를 기록하는 정보시스템에 액세스할 수 있어야 하며(Article §34;정보주체 접근권), 접근권이 있는 자가 자신에 대한 부정확·불완전한 정보 또는 기한이 지난 정보에 대해 수정 및 폐기를 요청할 수 있다(Article §36(1)정보의 정확성·완전성).

한편 의료정보에 대한 접근권은 제3자의 개입을 통해서만 행사할 수 있는 간접적 액세스권이라 할 수 있다.[193] 의료정보에 접근권을 행사하는 경우 그 정보는 지정된 의사를 통해서만 당사자에게 전달 할 수 있다(Article §40). CNIL은 이와 같은 개인정보취급과 관련되어 어떤 요청을 받으면 2개월 이내에 문제를 파악하여 필요한 조치를 취해야 한다(Article §28).[194] CNIL은 '개인에 관한 정보(les informations nominatives figurant)'[195]의 처리에 관하여 의견을 줄 수 있다. 국민은 누구든지 본인과 관계되는 정보가 정보처리의 대상이 되는 것에 대해 반대할 권리를 가진다(Article §26조(1)). 특히 인체유래물의 수집인 경우에는 명백한 동의를 얻어야 한다(Article §40-44). 다만 법률의 규정이 있거나 CNIL의 의견청취를 거친 개인에 관한정보의 자동처리에 대해서는 예외가 인정된다(Article §26(2); Article §15).

CNIL은 생존하는 개인에 대한 '개인정보 데이터베이스 등록제'[196]를 실시하고 있다.

---

193) 성낙인, 1998, 언론정보법, 서울, 나남출판: 584면 참고.

194) Article 28, Modifié par Loi n°2004-801 du 6 août 2004 - art. 4 JORF 7 août 2004.

195) Loi n° 78-17 du 6 janvier 1978; relative à l'informatique, aux fichiers et aux libertés, concernant les informations nominatives figurant dans des fichiers, toute personne a le droit de connaître les informations contenues dans un document administratif dont les conclusions lui sont opposées.; 개인에 관한정보; 개인으로 등록되거나 개인으로 용이 하게 식별할 수 있는 자연인에 대한 가치평가를 포함하거나 외부에 공개하면 당해 자연인의 프라이버시의 침해가 수반되는 문서를 말한다.

196) Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés Chapter Ⅲ, The Commission Nationale De L''Informatique Et Des Libertés)은 수집, 삭제, 재활용에 대하여 규정하고 있다. - 수집 : 정보는 역사적, 통계적 또는 과학적 목적의 처리

데이터베이스 등록제란 일정한 규모 이상의 개인정보나 민감정보를 수집하여 데이터베이스를 구축하고자 하는 자는 누구든지 개인정보를 수집하겠다는 사실을 사전에 통보하여 등록하는 것이다. 이렇게 일정한 목적으로 수집된 개인정보가 등록되어 있는 각각의 데이터베이스는 주기적인 감시를 통하여 개인정보의 유출을 사전에 예방하고, 애초의 목적으로만 사용되며, 목적 이외의 용도로 다른 데이터베이스와 결합하기 위해서는 일정한 요건을 준수해야한다.[197] 하지만 어떤 공공정보도 수집하거나 보유하지 않는다. 다만 공공데이터를 생산, 보유하고 있는 공공 및 민간기관과 국가 통계 및 다양한 분야의 연구를 위해서 사용을 원하는 기관 혹은 연구자와의 중재자 역할을 할 뿐이다.

CNIL은 개인정보를 수집·보유하고 있는 기관에 대하여 개인정보보호법규 준수여부를 감독하며, 정보처리 방법을 통보받는다. 정보처리법을 위반한 정보처리자(data controller)에 대해서는 5년간의 징역 또는 30만 유로의 벌금 등 다양한 제재 조치를 할 수 있다.[198] 그리고 개인정보처리에 관한 기준과 규칙

를 위하여만 그 정보가 수집되고; 삭제 : 삭제될 정보 유형 및 그 삭제요건은 그 정보를 생산하거나 취득한 기관과 기록보존 행정기관 사이의 합의에 의해 정해진다; 재활용 : 통계목적, 학문 목적 또는 역사연구 목적의 정보 재활용의 조건과 목적에 적합한 보존기간이 정해져야 한다.

197) 위의 법 제20조, 개인정보 데이터베이스의 등록;① 개인정보 데이터베이스를 보유하고자 하는 자는 다음 각 호의 어느 하나에 해당하는 경우에는 사전에 국가정보자유위원회에 등록하여야 한다. 1. 공공기관의 개인정보 데이터베이스 2. 대통령령이 정하는 업종의 개인정보 데이터베이스 3. 대통령령이 정하는 숫자 이상의 정보주체를 등록 대상으로 하는 개인정보 데이터베이스 4. 대통령령이 정하는 숫자 이상의 종업원을 고용한 자의 개인정보 데이터베이스 5. 대통령령이 정하는 개인정보를 수집하여 구축된 개인정보 데이터베이스 6. 대통령령이 정하는 기술을 사용하여 구축된 개인정보 데이터베이스; 제23조, 개인정보 데이터베이스의 결합 제한; 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 누구든지 자기가 수집·보관 하는 개인정보 데이터베이스를 공공기관이 처리하는 개인정보 데이터베이스와 결합할 수 없다. 1. 국가안전보장·사회질서유지 및 공공복리를 위하여 국가정보자유위원회가 필요하다고 인정한 경우 2. 정보추체의 동의가 있는 경우 3. 다른 법률에 특별한 규정이 있는 경우.

198) French criminal code, Article 226.17.1

개정의 권한을 가지고 있다. 현재는 공공부문의 특정 영역과 산업에 국한되어 있으나 전체 영역으로 확대하는 추세이다. 또한 정보주체인 개인의 접근권 및 정정요구권이 침해되지 않도록 하기 위하여 침해사례의 중재 및 제재를 통하여 전문적이고 포괄적인 피해구제를 담당하고 있다. 2011년의 불만사항은 6천여 건이 접수되었고, 이중에서 15%의 소송문제를 해결하였다. 법률운영을 신속하고 적시에 수행하기 위하여 정치, 사회, 경제, 윤리, 법적 요구를 반영한 여러 종류의 시행령을 만들고 있다.[199]

표 8. 2011년 CNIL의 주요 활동

분 류	건 수	전년대비 증가비율
심의건수 (Decisions & deliberations adopted)	1,969건	25.5%
시정고지 (Notifications on video-surveillance systems)	5,993건	37%
비디오 감시체계 통보 (Complaints for indirect right of access)	5,738건	19%
생체정보측정 장비 허가 (Authorizations on biometric devices)	744건	5.4%
지리위치 통보 (Notification on geolocation system)	4,483건	33.5%
감사 (Audits)	385건	25%
정보보호담당 공무원의 충원 (Organizations have appointed a Data Protection officer)	8,635건	25%
경찰 및 첩보 등을 위한 간접적 접근 (Requests for indirect access to Police and Intelligence records)	2,099건	12%

199) 국가안보를 위한 개인정보처리에 관한 시행령(Décret 79-1160 du 28 décembre 1979), 개인건강정보의 처리에 관한 시행령(Décret99-919 du 27 octobre 1999), 공공부문에서의 법적용에 관한 행정통첩(Circulaire du 23 mars 1993).

이 밖에 전 국민을 대상으로 2년 마다 한번 씩 앙케트 조사를 실시하여 개인정보에 대한 권리와 자유 및 CNIL의 역할을 홍보하고, 정보주체, 정보사용자, 정보처리자, 공공데이터 생산기관 등 모든 이해관계자들에게 상담, 자문, 교육을 실시한다. 또한 공공데이터 활용계획서 검토 및 제안 등의 역할도 한다. CNIL의 주요 활동은 표 8과 같다.[200]

5.1.4 미국

5.1.4.1 프라이버시법

1970년대 디지털 정보처리의 확산은 공공과 민간부문 모두에 걸쳐 정보프라이버시 침해에 대한 우려를 야기했다. 연방정부는 1974년 공공부문에서 프라이버시 법(Privacy Act)[201]을 제정하여 미국 연방 공공기관에 대하여 디지털 기록에 대하여 기록의 안전 및 비밀을 확보하고 정보의 안전 또는 완전성을 보장하기 위해 적절한 행정적, 기술적, 물리적 안전장치를 마련할 것을 규정하였다.[202] 동 법은 후에 '컴퓨터 매칭과 개인정보보호에 관한 법률'(Computer Matching and Privacy Protection Act)과 합쳐지면서 개정된다. '컴퓨터 매칭과 개인정보보호에 관한 법률'은 1988년 미 의회가 통과시킨 법이다.

1977년 미 연방정부는 정부공무원들의 개인정보를 모두 전자화하기 시작하였는데, 데이터베이스가 원래 수집 목적 외로 활용되었다. 그래서 공공기관이 준수해야하는 절차적인 요구사항을 규정한 것이다.[203] 개정된 프라이버시 법에서는 공공기관이

200) CNIL, 2001, Activity Report 2011, Paris, FRANCE: p. 4.

201) http://archive.opm.gov/feddata/USC552a.txt

202) France Belanger and Janine S Hiller, 2006, "A framework for e-government: privacy implications." Business process management journal No. 12(1): pp. 48-60.

203) Gary T. Marx, 1989, Undercover: police surveillance in America, Oakland, CA, University of California Press: pp. 180-234.

개인 정보를 담고 있는 데이터베이스의 존재를 공시하도록 하였다. 그리고 개인으로 하여금 자신의 기록을 접근하고 그 내용을 정정할 수 있는 기회를 제공하도록 하였다. 그리고 공공기관에는 '개인정보의 정확성, 적절성, 시의성 및 완전성을 유지할 의무를 부과하였다. 동 법률은 연방정부에 대한 개인정보보호를 규정하고 있어 다른 공공기관에는 적용되지 않아 공공부문에 대한 완전한 일반법으로 보기는 어렵다(5 U.S.C. §552(e)).

동 법은 개인정보의 수집기관이 필요한 한도에서만 정보를 수집 보유하도록 하고 가능한 본인으로부터 수집할 것을 규정하고 있다. 서면요청이나 사전 서명동의에 의하지 않고는 개인정보를 공개 할 수 없도록 하고, 다만 통계목적이나, 연방정부의 목적범위내의 통상적인 사용, 보관 목적, 법집행목적, 의회조사목적 기타 행정목적인 경우에는 예외로 하고 있다. 또한 제3자에 대한 제공은 원칙적으로 법률상 근거에 의해서만 허용되며, 이 경우 그 제공사실을 당사자에게 고지하는데 상당한 노력을 하도록 하고 있다(5 U.S.C. §552a(e)(8)).

미국의 공중보건데이터 표준 컨소시엄(Public Health Data Standards Consortium; PHDSC)에서는 개인건강정보의 이차 활용[204]이 효율적으로 이루어질 수 있도록 지원하기 위해 지침을 만들었다. 각종 정보 보호법과 지침에 관련된 자료를 취합하여 개인건강정보 등 공공보건 분야에서 활용하는 건강정보에 대하여 준수해야할 보호에 관한 지침[205]을 제시하였다. 이 지침에서는 특정한 건강정보에

204) 진료와 직접적으로 관계없이 개인건강정보를 사용하는 것으로 분석, 연구, 질·안전 측정, 공중보건, 지불, 공급자 자격 또는 인증, 마케팅, 기타 상업 활동 등이 여기에 해당함, 즉, 원래의 수집목적 이외의 목적으로 사용되는 것으로 진료와 직접적으로 관계없이 사용하거나, 환자가 받고 있는 진료를 지원하는데 직접적으로 관여하지 않는 목적으로 사용하는 것. Secondary uses and re-use of healthcare data, 2007: taxonomy for policy formulation and planning, American Medical Informatics Association.

205) Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule, NIH Publication Number 03-5388.

대하여 보건당국이나 의료제공자, 건강보험자가 공개의 주체라면 이차이용을 위하여 공개 할 수 있다는 특수 목적에 대한 당위성을 제시하였다. 즉 건강정보라 할지라도 이차 활용의 목적과 용도에 따라 분류[206]하여 연구의 정당성을 확보해야 한다. 연구의 정당성은 몇 가지 필요요건을 충족해야만 한다. 즉 최소한의 필수적 요구사항의 적용 가능성, 공개 요구에 대한 설명의 가능성, 특별한 다른 법률의 고려사항 적용의 가능성 등을 충족해야한다.

건강정보와 관련된 정보프라이버시는 헌법상의 프라이버시로서 보호하고 있다. 예를 들면, 병원이 목사가 의무기록에 접근할 수 있도록 허용한 것은 헌법상 프라이버시를 침해한 것으로 판결한 바 있다.[207]

5.1.4.2 정보자유법

정보자유법(Freedom of Information Act)에는 정부의 공공문서에 기록된 정보들을 공개하도록 강제하면서도 프라이버시의 보호를 위한 면제조항을 두고 있다. 즉 “공개하면 개인의 프라이버시에 대한 명백하게 부당한 침해가 되는 인사 및 의료에 관하 파일 기타 이에 유사한 파일”(5 U. S. C. §552(b)(6)), “법집행목적을 위하여 수집된 기록 또는 정보”로서 그의 제공이 개인의 프라이버시에 대한 부당한 침해가 될 것이 합리적으로 예측될 수 있는 경우를 말한다(5 U.S.C. §552(b)(7)(C)).

---

206) ①개인 식별 가능한 건강정보, ②정신건강, 화학·약물 중독, 성매개 전염병, 에이즈 관련 건강정보, ③생정통계, 전염병 등록, 질병 등록 등 공공보건정보, ④공공보건 프로그램 운영 및 평가, 테러리즘 대비, 질병발생감시, 보건서비스 제공, ⑤감염병감시, 손상, 장애의 예방 및 관리, 생정 통계, 식중독 보고, ⑥기타 (제한된 데이터 세트, 식별 불가능한 건강정보).

207) Carter vs. Broadlawns Medical Center, 667 F. Supp. 1269, 1987; Having carefully considered all the evidence, the Court finds that the employment of a chaplain at a tax-funded county hospital whose salary is paid for by tax revenues would violate the Establishment Clause of the First Amendment to the United States Constitution if that clause were viewed in isolation.

법원은 정보자유법의 면제조항을 근거로 국가가 보관하고 있는 정보의 공개를 거부할 수 있는가에 대한 이익형량의 기준을 '주된 목적(central purpose)'의 법리로서 제시하였다. '주된 목적'의 법리는 사생활 침해와 정보공개 분쟁에 관계된 판결들에 대한 유력한 분쟁해결의 판단기준으로 채택되었다.[208]

처음으로 제시된 판결은 'U. S. Dept. of Justice v. Reporters Committee for Freedom of the Press' 판결이다. 이 사건은 CBS 방송국과 기자협회가 법무부를 상대로 조직폭력배 4명에 관한 형사 기록을 요구한 데서 비롯되었다. 쟁점은 연방수사국의 컴퓨터에 있는 전과기록을 정보자유법의 면제조항 제7항(c)를 근거로 공개를 거부할 수 있는가였다. 즉 민감정보의 공개가 프라이버시를 부당하게 침해할 것으로 합리적으로 예상되는가가 핵심적인 관점이었다.

주요판단의 요지는 컴퓨터에 집적되어 있는 정보는 전과 기록뿐만 아니라 생년월일, 신체적 특징과 같은 사적인 정보를 포함하고 있으므로 실질적인 프라이버시 침해가 발생했다는 것이다. 그래서 당해 기록대장의 제3자 공개는 범주적으로 프라이버시의 부당한 침해에 속한다는 것으로 판결하였다.

이에 반하여 소수의견으로서 해당 행정기관의 행정서비스 결과로 얻어진 정보가 아니라 행정기관이 보유하고 있는 개인정보이기 때문에 사생활 보호의 이익이 사실 상 가장 큰 반면 일반대중의 정보공개 이익은 가장 약하다는 의견도 있었다. 그래서 사생활 침해는 아니라는 의견이었다. 이 판결은 어느 정도의 범위 내에서 공개할 것인지 그 정도를 고려했다는 점에서는 주목을 받았다.

5.1.4.3 유전자정보차별금지법

2008년에 제정·시행된 유전자정보차별금지법(Genetic Information Nondiscrimination

208) 김형준, 1999, "온라인 법률정보시스템의 구축에 따른 법적 문제- 정보공개와 사생활보호를 중심으로-", 법학논문집 제 23집 제2호: 124-126면.

Act)은 원칙적으로 환자와 시험대상자에 대한 전면적인 보호를 목표로 한다. 예를 들면 동의 과정에 유전학 또는 유전체연구 참여의 위험을 변경하거나 줄이는 것을 반드시 포함시켜야 한다고 명시했다.[209] 일부 주(State)법은 모든 종류의 유전자 검사에 대하여 동의를 요구하지만 이를 명시적으로 언급하지 않는 주(State)도 있었기 때문이다.

유전자 정보를 기초로 건강보험과 고용 상의 차별은 금지한다. 다만, 몇 가지 예외를 인정하고 있는데 이에 대해서 법 집행기구가 차별금지의 예외를 인정하는 것이 타당한 지에 대해서 광범위한 논의가 있었다. 동 법률의 취지는 연구는 보다 엄격하게 주, 지방, 국가 수준의 규정을 준수해야 한다는 것으로서, 예컨대 미 국립보건원의 규정과 같은 것을 말한다.

미 국립보건원의 규정에 의하면, 시험대상자의 개인식별정보는 데이터 저장소(genome-wide association study; 이하 GWAS)에서 공개되지 않도록 한다.[210] 그리고 기관심의위원회에서 연구목적을 위한 정보 공유에 대하여 정보제공자의 동의서의 내용과 일치하는지, GWAS 데이터 저장소에 제출한 정보와 관련된 개인, 해당 개인의 가족, 집단이나 인구집단에게 발생 가능한 위험이 고려되었는지 심사하고 입증하도록 하고 있다. 만약 기관심의위원회의 승인을 받은 연구계획서가 일부분이지만 명시된 연구목적이 아닌 불특정한 연구목적으로 데이터저장소에 인간 유전물질이 저장되어 있다면, 검체 제공자에게 별도의 동의서를 받도록 하고 있다.

미래의 연구에 대한 동의와 관련하여 발생할 수 있는 문제를 해결하기 위해서는 데이터저장소와 인간유전물질이 별도의 장소에 보관되어 있거나 혹은 각기 다른 공공기관에서 수집되었다면, 이를 통합하는 체계가 필요하다. 통합체

---

209) http://thomas.loc.gov/cgi-bin/query/D?c110:6:./temp/~c110T5d97r::

210) NIH Genomic Data Sharing Policy.
http://grants.nih.gov/grants/guide/notice-files/NOT-OD-07-088.html

계에는 정보 시스템의 연계뿐만 아니라 데이터처리의 일관된 절차가 포함되어야 한다. 따라서 특정기관과 특정 데이터베이스가 하나의 세트로 묶여 동의 및 심사·승인 양식이 법적 효력을 가진 형태로 개발해야 될 필요성이 높아지며, 이를 수행하는 독립적인 정부 기구의 역할을 고려해야만 한다.

5.1.5 캐나다

캐나다 온타리오 주의 '개인의료정보보호법(Personal Health Information Protection Act; 이하 PHIPA)'은 정보주체에게 명시적 동의와 묵시적 동의를 허용하고 있다. 이와 같은 점에서 사전에 서면 동의만을 허용하는 우리나라의 경우와 구별된다.

5.1.5.1 개인 의료정보보호법

2004년 캐나다의 온타리오 주에서 제정한 의료분야의 개인정보보호법이다. 의료시스템에서 개인의료정보를 수집·사용·공개하는 방식을 통제하며, 의료전문가로부터 개인정보를 전달받는 개인 및 기관을 규제한다. 이를 위해서 표준화 방법, 전문규정, 정책, 지침 등으로 성문화하였다. 그리고 환자가 자신의 의료정보에 접근할 수 있도록 환자의 권리를 확대하고 이 권리침해가 있을 경우에는 온타리오 주의 정보보호위원회(Office of the Information and Privacy Commissioner; 이하 IPC)를 통해 해결한다.

의료정보의 경우에는 정보 관리자 또는 해당 부서가 포괄적인 검토용 제안서를 제출받아서 개인식별자가 제거된 정보에 한해 공개를 결정한다. 단 공익이 있을 것으로 판단한 경우에 개인식별 정보를 최소화하여 공개를 허용할 수 있다.

캐나다의 정보보호위원회는 그 근거가 되는 주법에 따라 주마다 커미셔너를 두어 개인정보 및 정보주체의 권리를 보호하고 있다.

PHIPA에서 규정하고 있는 동의는 명시적 동의와 묵시적 동의로 이루어져 있다. 동의를 할 경우, 명시적인 동의나 묵시적인 동의나 모두 사실을 파악할 수 있는 상황이어야 한다. 즉, 정보관리자는 해당 목적을 설명한 통지를 개인이 주목할 수 있는 방식으로 게시 또는 열람할 수 있도록 하는 것이다. 정보주체는 수집·사용·공개의 목적을 파악하고, 또한 동의를 철회할 수 있다는 것도 알고 있어야 한다.

명시적 동의는 의료정보 관리자가 개인의료정보를 수집·사용·공개하도록 허락하는 명백하고 직접적인 동의를 의미한다. 구두, 서면, 전자매체 등 모두 가능하다. 명시적 동의가 필요한 특정한 상황은 의료정보 관리자나, 관리범위 밖의 개인 또는 기관에 공개할 경우다. 예를 들어 약사가 보험업체에 의료정보를 제공하는 것은 관리범위 밖의 제3자에게 제공한 것으로 추론되어 정보주체로부터 명시적 동의를 받아야 한다. 또한 의료정보 관리자가 의료서비스를 제공하거나 서비스 제공지원을 목적으로 다른 관리자에게 정보를 공개할 경우와 연구목적인 경우에도 명시적 동의를 받아야한다. 그리고 합법적으로 개인의료정보를 획득한 연구자들은 3년 간 계속해서 해당 정보를 사용·공개할 수 있다. 단 특정 조건 및 제한 사항을 두어 이를 충족한 경우는 예외로 한다. 예외조항에 해당하는 동의가 묵시적 동의이다.

묵시적 동의의 경우, 의료정보관리자는 합리적으로 판단하였을 때 개인이 자신의 의료정보를 수집사용 공개하는데 동의할 것으로 보이는 정황을 통해 이러한 동의를 추론할 수 있다. 의료정보 관리자가 직접 의료서비스를 제공할 목적으로 관리범위 내에서 관리자간에 정보를 주고받을 경우 묵시적 동의를 받은 것으로 허용한다. 하지만 만약 정보주체가 자신의 의료정보를 수집·사용·공개하지 않도록 특별히 요청한 경우에는 묵시적인 동의를 인정하지 않는다.

5.1.5.2 디자인에 의한 프라이버시보호(Privacy by design)

캐나다 온타리오주의 정보프라이버시 커미셔너인 케보키언(Ann Cavoukian)이 처음 소개한 '디자인에 의한 프라이버시보호(Privacy by design)' 개념은 네트워크에 연결된 대용량의 정보와 정보시스템의 발전과 그 영향에 따라 프라이버시에 미치는 영향을 분석하여 그에 따른 보호방법을 모든 유형의 개인정보에 적용할 수 있도록 일곱 가지 원칙을 제시하였다(표 9).

표 9. Privacy by Design 의 기본원칙

원 칙	내 용
사후대응이 아니라 사전대비 (Proactive not Reactive)	반작용적인 조치보다는 사전에 대비하는 것으로서 침해가 일어나기 전에 예측하고 방지해야 한다.
프라이버시 보호를 시스템의 기본 값으로 설정 (Privacy as the Default Setting)	정보주체가 특정한 조치를 하지 않아도 기본적으로 시스템이나 비즈니스 현장에서 개인정보가 자동적으로 보호되도록 해야 한다.
계획에 포함된 프라이버시 (Privacy Embedded into Design)	프라이버시 보호는 정보기술 시스템이 제공하는 주요기능의 본질적인 요소 및 비즈니스 운영설계와 계획에 포함되어 있어야 한다.
포괄적 기능성 보장 (Full Functionality)	모두에게 도움이 되는 상호보완적 방식으로 모든 합당한 목적과 이해를 수용해야한다. 보안과 보호라는 두 가지의 개념을 동시에 추구해야한다.
시작부터 끝까지 보안 (End-to-End Security)	정보를 수집하긴 전 시스템에서부터 보안이 이루어져야하며, 안전하게 수집되고, 정보생명주기의 마지막 단계에서 안전하게 삭제되어야 한다.
가시성과 투명성 (Visibility and Transparency)	어떠한 비즈니스 관행이나 기술이 포함되었든지, 필요시 별도의 검증 절차를 거쳐, 명시된 목적에 따라 이행되고 있다는 것을 모든 이해당사자들이 알고 있어야 한다. 구성요소과 운영절차를 투명하게 유지하고 검증과정을 거쳐야 한다.
프라이버시 존중 (Respect for User Privacy)	보안시스템설계자와 운영자가 프라이버시 보호를 위한 강력한 기본 설정, 적절한 알림, 사용자 선택사항에 대한 권한 등을 마련하여 사용자 중심의 제도로 운영해야 한다.

프라이버시 보호를 위한 시스템 설계를 지칭하는 'Privacy by design'은 프라이버시 보호를 위해서는 법과 제도를 따르거나 정보보안 강화를 위한 기술을 배포하는 것만으로는 부족하다는 반성에서 출발했다.[211] 말하자면, 프라이버시 보호를 위한 법제도의 운영에 있어서 기술적인 요소를 고려해야 한다는 원칙이다. 프라이버시 보호에 대한 확신은 첫째, 정보기술 시스템, 둘째, 책임 있는 조직운영, 셋째, 네트워킹의 인프라와 물리적인 디자인의 균형 있는 설계 등 세 부분에서 통합적이고 상호보완적인 원칙을 적용해야 한다는 것이다.

'Privacy by Design'의 개념은 미국 연방통상위원회(U.S. Federal Trade Commission)와 유럽위원회(European Commission) 등을 포함한 국제기구와 여러 나라에서 시스템디자인 원칙으로 채택되었다.[212] 2011년에는 'Privacy by Re-design'의 개념으로 확장시켰다.[213] 이 발전된 개념은 기존의 시스템과 프로세스를 새로운 개인정보보호의 기준에 맞추어 접근하였고, 시스템의 기능적인 면을 더 고안하였다. 이 새로운 개념에는 개인데이터생태계(Personal Data Ecosystem, 이하 PDE)라는 모델을 도입했는데, 페이스북, 구글, eBay와 같은 온라인 환경에서의 서비스와 그 조직에 대한 규율을 담고 있다.[214] 이 규제에서는 두 가지 핵심 기술 및 서비스 구성요소를 제안한다. 즉 개인 정보저장소(Personal Data Vault)[215]와 정보공유 플랫폼(data sharing platform)이다. 개인정보저장소는 개인이 자신의 정보에 대하여 수집, 저장, 사용,

---

211) Ann Cavoukian, 2009, Privacy by design. Take the Challenge. Information and Privacy Commissioner of Ontario, Canada.

212) Ann Cavoukian, January 2011, Privacy by Design, Ontario, Information and Privacy Commissioner.
http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

213) Ann Cavoukian, et al., 2011, Privacy by ReDesign: Building a Better Legacy. Ontario, Information and Privacy Commissioner: pp. 1-8.

214) Ann Cavoukian, 2012, Privacy by Design and the Emerging Personal Data Ecosystem, http://www.privacybydesign.ca/

215) Alternative terms used to describe a Personal Data Vault include: Personal Data Store, Personal Data Locker, Personal Cloud, and Personal Data Service.

공동이용, 접근권한 등을 스스로 컨트롤 할 수 있도록 권한을 부여하는 것이다. 무엇보다 안전하게 데이터를 공유하고 교환할 수 있도록 하는 것이 주목적이다. 즉 개인이 자신의 기준과 판단에 따라 자신의 정보를 밖으로 보내는 것을 관리하고, 다른 출처로부터 데이터를 요청함으로서 정보를 끌어올 수 있다.[216]

5.1.6 생체・의료정보 보호관련 외국 법제도의 비교

각국은 입법을 통하여 개. 법률제정을 통하여 어떠한 이익을 프라이버시로 보호하여야 할 것인지를 정하고, 개인의 권리를 보장하는 차원에서 개인정보를 보호하기 시작했다.

국제기구는 개인정보보호의 수집·이용·유지에 있어 준수해야 할 대부분의 원칙들을 규정하고 있으나, 그 적용대상이 정보의 저장·정보의 논리적 분석·수정·삭제 등을 위한 자동처리 방식에 따라 처리되는 데이터(any set of data undergoing automatic processing)에 국한되어 있다. 국제기구의 원칙은 개인정보보호법제의 표준안으로서 개인정보보호법을 새로이 제정하고자 하는 많은 국가들에 의해서 수용되었다. 다만 그 실행을 담보할 만한 초국가적인 법적 장치가 없다는 점이 한계로 지적되고 있다. 하지만 우리나라에서와 같이 분야별로는 상이한 목적을 위하여 이차 활용하지만, 이차 활용을 위해서는 다양한 공공정보를 공유하거나 연계해야할 필요성을 가진 공공기관이 단일하게 적용할 수 있는 규칙으로서 시사점을 도출할 수 있다. 특히 법적 구속력이 있는 공통의 규칙으로서 유럽연합 등에서 활용된다는 점은 공공기관 간의 정보이전을 위해 참고할 수 있으리라 생각된다. 국제기구의 민감정보 보호 원칙의 공통점과 그 내용은 표 10과 같다.

---

216) Martin Kuppinger, 2012, Life Management Platforms: Control and Privacy for Personal Data, Wiesbaden, KuppingerCole: p. 10.

표 10. 국제기구의 민감정보 보호 원칙의 공통점과 세부내용

원칙의 공통점	OECD Guidelines	European Conventions	APEC Framework
수집의 합법성	수집제한	정당성 확보	사전예방 수집제한
이용 목적의 제한	목적 명시, 이용 제한 비례적 사용 데이터 정확성	목적명시 이용제한 데이터의 품질 데이터의 정확성	개인정보 이용원칙 개인정보 통합원칙
데이터의 보안과 비밀성 보장	보안 및 안전 확보	비밀성 정보처리 보안	보안 및 안전 확보
이용에 관한 투명성	공개	정보처리에 관해 정보주체 참여	개인정보수집에 대한 고지
정보주체의 권리	정보주체 보호	접근권, 정정 요구권, 삭제요구권	접근권 혹은 정정권 선택
정보처리자의 책임	책임성	법적구제 책임성	책임성
민감정보 분류	수집제한	동의	동의
이차 활용	최소처리 최소이용	이용 제한	최소처리 최소이용

유럽연합은 각 회원국 간의 자유로운 개인정보 유통을 위하여 지침과 규칙, 행동강령 형태의 기준을 마련하고 있다. 이러한 실행규칙은 구속력이 있어 각 공공기관이 다른 법률에 근거하여 이차 활용을 할 때 발생할 수 있는 문제에 대한 개선방안으로서 활용될 수 있을 것이다. 자발적이고 구속력 있는 개인정보보호 규칙으로서 제3자에의 정보이전을 위한 안전조치를 인정하는 APEC의 CBPR[217]과 유럽

217) APEC 2012/SOM1/ECSG/DPS/I/009 Agenda Item 6, Submitted by United States,

연합의 BCR을 비교하여 표 11과 같이 정리하였다.

표 11. APEC의 CBPR 과 EU의 BCR 비교

	APEC CBPR	EU BCR
계약원칙	사전예방	공개, 투명성
	고지	목적제한
	사용	개인정보와 민감정보 구분
	수집제한	데이터의 질
	선택	개인정보처리권
	보안지침	계약에 의한 보안
	통합	보유의 정당성이 없는 데이터 삭제 의무
	접근권 및 정정권	접근권 및 정정권
	책임성	계약 이후에 전송
법률적용에 관한 규칙	기업은 불만 처리를 할 수 있어야 함	계약을 하는 기관들은 불만 처리를 위한 내부 담당자가 있어야함
	기업은 분쟁해결을 할 수 있어야함	제소하기 전에 정보보호기구[218]에서 불만이 해결되어야 함.
	CBPR 요구사항의 적용효과가 나타나도록 법률이나 규정 제·개정	정보보호기구와 기업은 협력해야함. 기업들은 해당국가의 개별법률에 따라 BCR을 적용함
정보보호 의무대상	내부: 기업과 승인된 조직과 제3자, 정보처리자	내부 : 그룹마다 참여기업의 모든 그룹
	외부: 책임자와 정보보호기구	외부: 기업
정보보호 책임 추적	제3자에 의한 '책임성' 재검토	감사제도 (BCR의 계약 내용 점검 포함) 직원에 대한 데이터 보호에 교육프로그램 개인정보보호 담당자들 간의 네트워크
계약 신청 범위	요구사항 중에서 선택할 수 있음	비유럽연합국가에서 유럽연합국가로 데이터전송을 할 수 있는 솔루션제공
	제3자에게도 확대할 수 있음	(i)기관차원 (ii)개별정보차원 중에서 선택
책임의 유효기간과 대상자	CBPR 인증된 기업	원칙: EU내의 기업 대체가능한 책임자: 데이터요청자와 수신자간의 공동책임

Commission nationale de l'informatique et des libertés.

218) Article 29 Data Protection Working Party, Recommendation 1/2007 on the Standard

유럽연합 국가들과 미국은 일반적으로 개인정보보호의 정도를 달리하여 더 민감한 정보에 대한 수집과 이용에 대해서는 매우 구체적으로 명시해놓고 있었다. 민감정보의 안전한 이차 활용과 관련된 법조항으로는 표현방식의 차이는 있지만 모두 정확성의 원칙과 목적 구체성의 원칙, 공개의 원칙을 구체화하고 있었다. 민감정보에 대한 수집금지는 본인의 동의, 법률의 규정, 중대한 공익을 위하여 필요한 경우에 있어서 예외를 허용하는 공통점이 있었다.

다른 점으로는 유럽식 모델에서는 프라이버시에 대한 관점이 다른 이익보다 우선하는 기본적인 권리로 해석하지만 미국식 모델에서는 상업적인 거래의 효율성을 고려한 균형 잡힌 프라이버시 보호를 법제도의 원칙으로 삼고 있었다. 따라서 정보보호기구가 하는 일도 유럽식은 입법, 행정, 사법권으로부터의 독립성을 강조하지만 미국식은 그렇지 않았다. 우리나라는 민간과 공공부문을 통합하여 일반형 기본법으로서의 개인정보법제를 시작하였지만, 개별분야에서 특별법이 제정되어 개인정보를 활용하도록 하고 있다는 점에서 유럽과도 차이를 보인다.

프라이버시 보호를 위한 시스템 마련을 위해서는 캐나다의 'Privacy by Design'을 주목할 필요가 있다. 시스템을 디자인하는 초기 단계에서부터 프라이버시 보호기능을 내장하여 설계하는 것이다. 시스템의 설계는 의료기기와 연결되어 있는 등록정보 시스템에 오류 없이 생체·의료정보가 수집·관리될 수 있도록 데이터 안정성과 적시성을 최우선 목표로 해야 한다. 그리고 이차 활용을 목적으로 전송하기 위해서는 데이터를 전송하는 장치 간에 동일한 기능이 구비되어 있어야

Application for Approval of Binding Corporate Rules for the Transfer of Personal Data, Adopted on 10 January 2007, Data Protection Authorities(DPAs) ; 유럽의 정보프라이버시는 '데이터보호'에 있다. 따라서 개별회원국의 독립적인 데이터보호기구(DPA)에 의해 BCR의 승인을 얻는 과정을 간소화하고, 그 양식을 BPR이라는 하나의 양식으로 통일하였다. 따라서 DPA의 권고는 다른 모든 선택보다 우선하고, 최후의 결정권을 갖는다.

한다. 또한 사후 동의 절차를 계획할 경우 처음부터 개발자가 고려해야 할 문서, 형식, 동의 개정 및 재승인, 규제요건 등을 적용할 필요가 있다.

5.2 생체·의료정보 이차 활용을 위한 외국 법제도 비교분석

5.2.1 국제기구

5.2.1.1 유네스코 인간유전자 데이터에 관한 국제선언

UNESCO에 의해 2003년에 제정[219]된 인간유전자 데이터에 관한 국제선언(International Declaration On Human Genetic Data)은 1997년 인간게놈과 인권에 관한 보편선언(1997, Universal Declaration on the Human Genome and Human Rights)으로 부터 인간게놈 데이터와 관련된 사항을 국제선언으로 채택한 것이다. 이 선언 14조는 유전정보 처리 시 유전자 프라이버시권 보호와 비밀성에 관하여 규정하고 있다.[220] 구체적인 내용은 다음과 같다.

(1) 인체유래물은 중요한 공공의 이익을 위하여 국제 인권법에 부합하는 국내법에 의해 제한적으로 허용될 수 있다. 식별 가능한 개인, 가족 또는 적절한 그룹에 연결된 인간 유전자 데이터의 기밀성을 보호하기 위해 노력해야한다.
(2) 인간 유전자정보, DNA 검사정보, 인체유래물 시료 등은 사전 동의를 얻은 경우를 제외하고는 공개되거나 제3자 특히 고용주, 보험회사, 교육기관과 가족 등에게 접근가

219) International Declaration on Human Genetic Data, 2003, 32nd General Conference. UNESCO.
220) Records of the General Conference 32nd Session Paris, 29 September to 17 October 2003, UNESCO, Article 14: Privacy and confidentiality.

능하게 되어서는 안 된다. 연구대상자의 명시적 동의는 국내법과 국제법을 모두 준수해야 한다. 연구대상자의 프라이버시는 보호되어야하고 데이터는 기밀로 취급되어야한다.

(3) 인간 유전자정보, DNA 검사정보와 의생명과학연구의 목적을 위해 수집된 인체유래물 시료는 일반적으로 식별 가능한 개인정보와 링크 할 수 없다. 그러나 이와 같이 링크가 안 되는 경우에도 필요한 정보보안 조치와 시료의 보안을 보장해야한다.

(4) 인간 유전자정보, DNA 검사정보와 의생명과학연구의 목적을 위해 수집된 인체유래물 시료는 필요한 경우 식별할 수 있는 개인정보와 연결된 상태로 남아있을 수 있다. 단, 연구 목적에 한정하고 개인정보의 기밀성과 개인정보보호와 관련된 국내법에 따라 보호된다.

(5) 인간 유전자정보, DNA 검사정보는 수집, 처리를 위한 목적을 달성한 후에는 더 이상 식별 가능한 형태로 보관되어서는 안 된다.

이 선언에서 주목할 것은 의생명과학연구 목적에 한정하여 식별가능한 개인정보와 시료를 함께 보관할 수 있다는 것이다. 현실적으로 연구를 위해서는 인체유래물과 이들에 대한 정보의 맵핑이 필요한 경우를 반영한 내용이라고 볼 수 있다.

2014년 제 21차 국제생명윤리위원회의[221]에서는 2005년에 유네스코가 승인한 '생명윤리와 인권에 관한 보편선언(Universal Declaration on Bioethics and Human Rights)'의 제 15조 '이익공유(sharing benefit)' 원칙에 관한 개정을 논의하였다. 과학적 지식은 모든 인류의 소유물이며 특정개인의 재산권이 아니라 공공선이며 동시에 인권이다. 따라서 과학적 지식의 혜택도 권리로서 보장되어야 하는 사회적 책임임을 확인하였다. 이는 비밀성이나 기밀유지와는 상충되지만 과학적 연구나 기술개발의 혜택은 공익으로서 모든 인류에게 혜택이 고루 나누어져야 한다는 원칙에 관한 논의였다. 생체·의료정보를 활용하는 의생명과학연구가

221) 21st Session of the international Bioethics Committee of UNESCO, 9-10 September 2014. UNESCO Headquarters.

그만큼 많아지고 있고, 그 혜택도 보편적이 되어 가고 있는 국제사회의 흐름과 책임을 반증한다고 할 수 있다.

5.2.1.2 EU Directive 95/46/EC 의 포괄적 동의

유럽은 바이오뱅크에서 충분한 설명에 의한 동의가 갖는 문제점을 인체유래물을 공여할 시점에서는 미래 연구목적을 모두 예상할 수 없다는 점과 추가 동의를 받기 어렵다는 것에서 찾는다. 그래서 공여시점에서 '포괄적 동의(broad consent)'를 받는 방향으로 법 개정이 진행되고 있다. 하지만 포괄적 동의는 전면적 동의는 아니다. 구체적으로 말하자면, 사후거부방식으로 정보주체는 자기정보결정권을 행사할 수 있다. 정보주체가 행사하는 정보처리에 대한 '거부권(right to object, 제14조)'은 다음과 같이 정의 된다.[222]

> "정보주체는(a) 적어도 [공공기관이나 민간기관이 자신의 정당한 업무수행을 위하여 동의 없이 합법적으로 개인정보를 처리할 수 있는 경우에(제7조 e호; f호)], 언제든지 자신의 특별한 상황과 연관된 불가피한 정당한 사유를 제시하면서 자신에

222) EU Directive 95/46/EC - The Data Protection Directive, Article 14. The data subject's right to object Member States shall grant the data subject the right: (a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data; (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses. Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

관한 정보의 처리를 거부할 수 있는 권리를 가진다. 다만, 회원국이 국내법으로 이와 달리 규정할 수 있다. 정당한 거부가 있는 경우에, 당해 개인정보처리기관이 하고 있는 정보처리에서 거부 요청된 정보가 더 이상 포함되어서는 안 된다."

포괄적 동의를 인정하는 원칙은 다음과 같다. 첫째, 공여시점에서 미래의 연구 내용을 확정할 수 없을 지라도 연구가 이루어질 분야에 대한 최대한의 정보를 제시한다. 둘째, 수집된 인체유래물은 바이오뱅크 윤리위원회의 판단에 따라 활용된다. 셋째, 자신의 공여한 시료를 폐기 할 수 있는 권리를 보장한다.

이러한 포괄적 동의 혹은 사후 거부권을 통하여 정보주체의 동의 없는 제3자 제공을 개인정보 처리자 또는 제3자의 정당한 이익을 달성하기 위하여 필요한 범위 내에서 넓게 인정하고 있다.[223] 사후 거부권은 개인정보를 삭제하거나 처리 정지를 할 수 있는 권리로 보장된다고 볼 수 있다. 하지만 이 권리가 사전에 충분한 설명에 의한 동의가 면제된 연구대상자들에게 사후 거부권을 행사하는 방법으로 적용할 수 있는지는 더 따져볼 필요가 있다. 왜냐하면, 동의 면제된 정보 주체는 포괄적 동의조차도 하지 않았으므로, 사후 거부권이라는 권리 자체가 성립되지 않기 때문이다.

5.2.2 프랑스

5.2.2.1 건강 분야 연구 및 수집된 데이터의 처리에 관련된 법[224]

프랑스는 민감정보에 대한 법률을 별도로 제정하여 수집, 삭제, 재활용에 대한 합법성 조건을 규정하고 있다. 동 법은 목적 구속의 원칙을 적용하여 수집된

223) Timothy Caulfield, 2007, "Should donors be allowed to give broad consent to future biobank research?", KLJ 18: p. 209

224) Code de la santé publique, article L 1111-7, article L 1110-4, article R111-1 à 1111-8.

목적과 부합하지 않는 경우 정보처리를 금지한다. 그러나 통계 또는 학문, 역사 목적의 처리에 대하여는 예외를 허용하고 있다. 예외를 적용하기 위해서는 합법성, 사전에 익명화 처리, 익명화 처리 책임자의 의무 사항, 그리고 정보주체의 사용 동의, 정보 이전에 대한 거부 등의 조건을 충족해야 한다.

1994년 7월 1일의 개정법에서 보건 분야연구를 목적으로 하는 개인정보의 자동처리에 관한 사항이 신설되어 개인의 치료 목적으로만 정보이용이 허용되었다. 연구목적인 경우 일정한 조건이 있고 CNIL의 승인을 받아야 하며, 암호화한 후 전송할 수 있다.

1999년 7월 법 개정을 통하여 개인정보처리에 관한 예외조건으로서 보건의료 연구라는 목적[225]에 따른 예외 규정을 만들고, 치료에 대한 평가 목적을 위해 사용되는 조건[226]을 설정하고, 해당 데이터란 무엇을 지칭하는지 정의하였다.

2002년 3월 4일에 EU 지침을 반영하기 위하여 개정된 법률은 치료와 예방 활동의 평가나 분석을 위한 개인의 건강정보의 처리를 허용하는 내용이 새로이 마련되었다. 즉 환자의 권리와 의료 시스템의 품질 및 치료의 연속성을 보장하기 위해 또는 최상의 지원을 결정하기 위하여 의료 전문가는 환자에 대한 정보를 공유 및 교환할 수 있도록 하였다. 이에 따라 다른 법률 및 행정명령과의 관계(Article §29(1))를 조정하고 제4장의 적용방법에 관한 명령(Article §33(1))에 관한 규정이 신설되었다. 이 경우에도 법적 측면의 전제조건, 기술적 측면의 데이터 처리, 운영방식이 명시되어있다.

2004년 8월 6일에 대폭 법 개정을 통하여 '디지털 세상에서의 자유와 개인정보보호'라는 슬로건 아래 개인정보자기결정권 행사에 관한 문제를 해결하기

---

225) 보건의료연구목적 : 예방의학, 의학적 진단, 보건행정 목적에 필요한 정보, 국가통계위원회의 동의를 거친 통계목적의 정보, 역학, 모니터링, 임상 시험, 공중보건, 의학연구 목적의 정보(동 법률 제 9장에 규정된 형식에 부합할 경우).

226) 환자에게 의료 지원을 쉽게 한다거나, 의무적인 건강 보험 또는 공중 보건의 목적 등 환자에게 직접적인 혜택을 결정하는 조건.

위하여 CNIL은 직접 관여한다(To guarantee the right of access).[227]

2006년 10월 프랑스 정부는 국민 개개인의 사회보장번호(numero d'inscription au repertoire, 이하 NIR)[228]사용에 대한 워킹그룹을 설립하였다. 의료 연구 목적이나 다른 특정 권한이 필요할 경우, CNIL에 사전 요청하여 승인을 얻는 절차를 수행하기 위해서였다. 이때 다른 공공기관으로부터 획득한 정보와 NIR의 사용 여부를 통지해야한다.[229] 미리 정해놓은 각각의 목적과 사회보장기관과 해당 영역 및 특정한 조건 등을 이 워킹그룹에서 정하게 되는데, 그 구성원은 CNIL의 위원과 환자, 단체, 인권연맹, 보건전문가, 산업보건 전문가, 익명화전문가로 구성하였다.

2007년에는 의학연구에 활용되는 정보에 대한 감독과 동의서에 관련된 역할과

---

227) CNIL, Activity Report 2011, Paris, Commission nationale de l'informatique et des libertés: pp. 1-75.

228) 국가 자연인 식별자 저장소(Répertoire national d'identification des personnes physiques ; RNIPP)에 등록되어 있는 번호로서 프랑스에서 태어난 사람들의 출생기록이다. 2009년 기준 97.1백만명이 등록되어 있으며, 관리주체는 국가 통계연구소이다. NIR은 사회보장분야에서 처음으로 사용되었고, CNIL은 이 번호를 사회보장분야에 관련된 파일과 함께 저장할 있도록 승인하고 있다.

229) 연구자 및 의료 연구기관, 공중 보건당국은 원칙적으로 NIR 를 사용할 수 없다. 다만, 의료 및 보건 연구는 NIR의 기술적 프레임워크가 허용하는 법적 조치를 취할 때 가능하다.; ① CNIL은 연구자 및 보건 당국이 NIR을 사용 할 수 있도록 모든 이해 관계자 간의 협력과 조건이 명시된 컨텍스트를 정의한다. ②CNIL의 개인정보사용 결정 기준은 건강 데이터의 개인 정보 및 권리를 보호하면서도 의료 연구 및 공중 보건의 평가를 용이하게 한다는 기준의 합치여부이다. ③이미 구성된 NIR을 특수문자로 시리즈 화하여 단일 번호로 각 개인에게 할당하고, 가장 중요한 요소는 각기 다른 기관 간 전송과 이를 상호 연결을 할 때인데, 이를 위하여 특정분야(조세, 교육, 은행, 경찰 등)를 정하고 각 분야마다 식별자를 다르게 한다. ④특정분야 마다 개인정보처리자(data responsible treatment)가 각 기관마다 있어야 하며, 이 데이터의 '중복', '충돌', '오류연결'에 대한 안정적인 표준화된 기술적 솔루션을 실행해야 한다. ⑤일정한 숫자(60만 명)이상의 인구에 대한 특정한 연구에서는 발생할 수 있는 문제와 해결방법이 명시 되어야한다. ⑥CNIL은 NIR의 바람직한 사용 및 개인정보 보호를 위하여 새로운 ID를 부여한 건강데이터를 새롭게 만드는 것을 고려하고 있으며, 이러한 코드 변환을 승인하고, 사후 검증한다.

규제를 만들었다. 기관심의위원회는 '개인건강정보의 처리의 적법성'과 관련하여 CNIL과 사전상담을 한 후 심사해야한다.[230] 예를 들면 개인건강정보는 다른 정보들과 구별하여 정보시스템 안에 보관되어야 하고, 각 기관은 어떻게 이를 실행할 것인지 그 방법을 CNIL에게 알리고 승인을 받아야 한다. 정보를 공유하는 기관은 표준화된 측정기준과 평가방법이 적용된 정보처리방안을 마련해야한다.

5.2.2.2 공공기관의 행정문서 접근 위원회

행정문서 이용법률[231]을 근거로 1978년 설립된 공공기관의 행정문서 접근 위원회 (La Commission d'accès aux documents administratifs; 이하 CADA)는 모든 행정문서에 대해 공공기관 간 전송할 수 있는지 그 여부를 결정한다. 모든 정보공개는 개인에 관한 정보인가, 아니면 개인에 관한 정보가 아닌가에 따라 달리 시행된다. 개인에 관한 정보인 경우에는 제3자에게는 공개청구가 허용되지 않고 정보주체만 열람 청구할 수 있다. 개인에 관한 정보일지라도 일부 의료정보와 산업정보는 정보주체에게조차 열람이 금지된다. 개인의 의료정보는 청구인에게 직접 공개하지 않고 청구인이 지정하는 의사에게 공개하도록 한다.

CADA는 2005년부터 목적 외 이용을 위해 공공정보의 재사용 허용에 대한 심의를 하고 있다. 이때 제공되는 공공정보에 대한 이차 활용 가능성과 조건을 판단하고, 공공정보의 이차 활용을 향상시키기 위해 정부에 개정안을 제안하기도

230) Décret n°2007-1220 du 10 août 2007 relatif au prélèvement, à la conservation et à la préparation à des fins scientifiques d'éléments du corps humain et modifiant le code de la santé publique.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000829163&dateTexte=

231) Loi n° 78-753 du 17 juillet 1978, '행정과 국민의 관계를 개선하기 위한 조치들과 행정적 사회적 재정적 성질을 가지는 규정들에 관한 법률': LOI n° 78-753 du 17 Juillet 1978, Loi portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

한다. 정보주체가 소송을 원할 때는 국민 개개인을 대신하여 소송문제를 해결하고 권리구제를 한다.[232]

5.2.3 미국

미국에서는 개인정보의 이차 활용과 관련하여 '추가 동의 획득'의 여부가 뜨거운 쟁점이다. 지금까지 정리된 입장은 바이오뱅크의 효율적인 운영을 위해서는 보관중인 인체유래물과 기증자를 연결 할 수 없을 정도로 익명화가 되었다는 전제하에서는 추가동의 획득절차를 생략해도 좋다는 것이다. 하지만 추가 동의의 필요성에 대한 논의가 가열되자 익명화에 대한 개인식별가능성(identifiability) 논의로 대체했다는 비판이 있다.[233] 즉 바이오뱅크를 통한 연구를 수행할 때 추가 동의가 이루어지기 어렵다는 연구자의 입장을 지나치게 적극적으로 반영한 결과라는 것이다. 그래서 익명화방법에 대한 논쟁이 오히려 계속되고 있다. 왜냐하면 바이오뱅크에서 수행되는 연구들은 어떤 형태로든 기증자와 인체유래물을 연동하여 분석할 필요가 있기 때문이다.[234]

5.2.3.1 미국 경기회복 및 재투자법

'미국 경기회복 및 재투자법(American Recovery and Reinvestment Act of

---

232) CADA, 2012, Rapport d'adtivité, Paris, Commission d'accès aux documents administratifs: pp. 47-62.

233) Bernice S. Elger and Arthur L. Caplan, 2006. 'Consent and Anonymization in Research Involving Biobanks'. EMBO Reports 7(7): pp. 661-666.

234) 실제로 스웨덴에서는 해일로 사망한 사람들의 신원확인을 위해 사망자 중 바이오뱅크에 인체유래물을 공여한 사람들의 경우 그 시료를 사용하여 신원을 확인하는 것이 정당하다는 판단이 이루어졌다.

2009; 이하 ARRA 2009)'은 사회간접자본 건설 프로젝트, 의료보험, 재생 에너지 개발 및 일반가정의 세금 감면 혜택을 부여하는 것 등을 주요 목적으로 제정되었다. ARRA 2009의 하위법인 '경제적·임상적 건전성을 위한 건강정보기술법(The Health Information Technology for Economic and Clinical Health; 이하 HITECH)'[235]은 보건·의료 정보화에 범정부 예산투자 지원을 보장하고 있다. HITECH를 더욱 강화하고 병원 및 의사가 임상의사결정정보 시스템을 활용한 결과를 전자의무기록에 포함할 것을 규정하는 '환자보호와 적정진료법(Patient Protection & Affordable Care Act 2010)'를 제정하여 전자처방 및 전자 의무기록을 환자에게 제공할 수 있는 근거도 만들었다. 이는 보안이 보장된 개인전자건강정보의 교환과 이를 통한 보건의료의 질과 안전성 및 효율성을 개선하기 위함이다. 적격성이 인정된 병원이 이를 적용하는 경우, 메디케어와 메디케이드의 인센티브를 지급하도록 하고 있다.[236]

원활한 정책 시행을 위하여 국가 기술코디네이터사무국(Office of National Coordinator for HIT; 이하 ONC)을 설립하여 주요 인증표준기준을 제정하고 있다.[237] ONC는 미래 보건·의료 신기술의 지속적인 도입과 시장 확대 등을 통해 건강정보 활용체계 구현을 지원할 수 있는 의료기술 포털[238]을 구축 하고 전략 프로그램을 추진하고 있다.[239] 특히 행정부 또는 주정부에서 선정한 측정항목의 결과를 보고하기 위해서는 인증 받은 전자의무기록을 사용하도록 하고, 이러한

---

235) Health Information Technology for Economic & Clinical Health(HITECH)는 건강증진을 위한 보건·의료 기술을 의미 있게 활용하는 헬스케어 시스템의 도입을 위하여 경기부양 예산의 일부인 약 270억 달러를 2019년까지 투자하기 위해 제정되었다.

236) Medicaid Electronic Health Record Incentive Payments for Eligible Professionals. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MLN_MedicaidEHRProgram_TipSheet_EP.pdf.

237) http://www.healthit.gov/policy-researchers-implementers/about-certification

238) http://www.healthit.gov/

239) ONC, 2013.6. Federal Health IT Strategic Plan Progress Report.

인증된 방법을 사용할 경우에는 인센티브를 지급한다.[240] 이와 아울러 정보교환을 위한 재정 및 기술지원을 비롯하여 설명서를 제작하고, 실행 모델을 지원한다. 그리고 전자의무기록 교환이 진료에 새로운 증진을 가져오는 결과를 보여주는 병원과 의사, 그리고 의료소비자가 함께 참여하는 커뮤니티 프로그램을 진행한다.

5.2.3.2 건강보험 이전과 책임에 관한 법률

건강보험 이전과 책임에 관한 법률(Health Insurance Portability and Accountability Act 1996, 이하 HIPAA)는 연방 의회나 행정부가 프라이버시 규칙을 제정하도록 요구하였는데, 1999년 10월 연방 의회가 자체 부여한 최종시한을 넘겨 클린턴 행정부는 의료정보를 보호하기 위한 최초의 연방 프라이버시 규칙을 제안하였다.[241] 보건관련 기관 및 보험사에서 사용하는 개인정보의 보호에 대한 규정이다. 즉 직장이 바뀌거나 실직 등의 사유로 보험을 변경할 필요가 있는 경우, 건강정보 제공시 발생할 수 있는 개인정보의 침해가능성에 대한 보호 법률이다.

---

240) 인증요구사항; 전자처방(Computerized Provider Order Entry), 질 관리 보고, 임상의사 결정지원(CDSS) 규칙시행관리, 보험청구적정성검사, 전자청구서제출, 암호화(Encryption), 건강정보의 전자사본조회 및 발급, 검사결과, 퇴원요약의 전자사본 조회 및 발급 등. http://www.cms.gov/EHRIncentivePrograms

241) George J. Annas, 2003, "HIPAA Regulations – A New Era of Medical-Record Privacy?", The new england journal of medicine 348(15): pp. 1486-1490 참조; 이 제안은 다음 몇 가지 사항을 강제한다. 첫째, 환자들은 어떻게 정보가 사용, 보관 및 공개되는지에 관하여 명백한 서면 설명을 받아야 한다. 둘째, 환자들은 그들의 기록에 대한 사본의 획득과 수정을 요구할 수 있어야 한다. 셋째, 환자들은 정보가 공개되기 전에 그 권한을 주어야 하며 공개에 대한제한을 요구할 수 있어야 한다. 넷째, 정보제공자와 건강계획은 치료가 행하여지기 이전에 환자로부터 포괄적인 동의(blanket approval)을 요구할 수 없다. 다섯째, 건강정보는 몇 가지 예외를 제외하고는 건강의 목적 자체로만 활용될 수 있다. 여섯째, 정보제공자와 건강계획은 반드시 서면 프라이버시 절차를 채택하고, 고용인을 교육시키며, 프라이버시 관리인을 지정하여야 한다.

2003년 식별가능한 개인건강정보의 보호에 관한 표준(Standards for Privacy of Individually Identifiable Health Information)을 정하였는데, 이 규칙에서는 적용대상기관(의료보험자·의료제공자·의료정보전달기관), 보호되는 정보(개인식별 의료정보), 보호되지 않는 정보(개인익명화 정보), 의료정보의 이용과 제공 등에 대한 원칙[242]을 다음과 같이 마련하였다.

(1) 환자의 의료정보에 대한 3가지 권리(개시청구권. 정정청구권. 설명보고권)
(2) 환자 프라이버시 침해 시 민·형사 처분
(3) 공중위생·의학연구 등 국가적 우선사항에 대한 프라이버시권의 공적 의무
(4) 의료정보 중 환자의 신원정보 사용의 의료목적 내 제한
(5) 의료정보 수탁기관의 프라이버시 보호시스템 및 절차 수립

이 원칙에서는 특별히 동의를 요하지 않고 이용 또는 공개 할 수 있는 개인 진료정보의 범위를 상세히 규정하고 있다. 보건의료체계의 효율성과 효과성을 향상시키기 위한 목적이었으므로 건강관련정보와 개인 식별 보건의료정보(Individually Identifiable Health Information)[243]를 구분하고 있다.[244]

표 12에 표시된 18개의 항목이 HIPAA에서 규정하고 있는 '보호된 건강정보(Protected Health Information; 이하 PHI)'이다. 18개의 PHI는 무단으로 공개, 사용, 접근하는 것을 방지하기 위하여 익명화되어야 할 정보이다.

---

242) 백윤철·김상겸, 2006, 미국의 의료정보보호에 대한 연구, 고양, 한국학술정보: 77-87면.
243) HIPAA 제2편, 제 F부 제1171조.
244) HIPAA Privacy Rule 45 CFR §160, §164; 개인의정신적, 육체적 건강 및 상태에 대한정보(과거, 현재, 미래포함), 개인에게 제공된 의료서비스, 제공된 의료서비스 비용에 관한정보(과거, 현재, 미래포함)가 개인을 식별할 수 있는 항목을 포함할 경우.

표 12. HIPAA에서 제시한 완전히 제거해야 될 개인 식별자

1	이름
2	시군구 우편번호 및 그와 동등한 지역번호
3	생년월일, 입학일, 졸업일, 사망일, 개인과 관련된 날짜의 모든 요소
4	전화 번호
5	팩스 번호
6	이메일 주소
7	사회보장 번호
8	진료기록 번호
9	건강보험 수급자 번호
10	은행계좌 번호
11	면허증 번호
12	자동차등록번호와 자동차식별항목 및 고유번호
13	의료기기 식별항목 및 고유번호
14	Web URL
15	인터넷 프로토콜 (IP) 주소
16	지문, 음성등 생체 측정 정보
17	얼굴 전체 사진 및 이와 유사한 사진
18	유일한 번호, 특징, 기호

PHI를 '익명화'하기 위한 방법은 두 가지이며(§2(i)) 그 대상기관은 병원과 공공 및 민간 보험사이다.[245] 첫 번째 방법은 '세이프하버 방법(Safe Harbor Methods)'이다. 이 방법에 의해 개인 또는 개인의 친척, 고용주, 또는 가족 구성원의 식별자들은 제거된다. 이때 하나의 정보로 개인을 식별할 수 없음은 물론이고 두 가지 이상의 정보를 조합하여 개인을 식별하는 것 또한 불가능해야한다(HIPAA §164. 514).

두 번째 방법은 '전문가 결정 방법(Expert Determination Methods)'이다.[246]

245) 익명화(anonymous data)는 직업, 주거형태, 교육수준, 소득수준 등 맥락적 변수까지 고려하여 개인을 식별하지 못하도록 한 것으로서 보건의료정보(PHI)라 할지라도 익명화를 위한 표준과 실행요건을 충족하는 경우에는 동 법 및 동 규칙의 규율대상이 아니다.
http://healthcare.partners.org/phsirb/hipaaglos.htm

246) Guidance on De-identification of Protected Health Information November 26, 2012.

이 방법은 개인을 식별할 수 없는 형태로 전환하는 통계적 혹은 과학적 원칙과 방법에 대하여 합리적 지식과 경험이 있는 자가 그러한 원칙과 방법을 적용한 결과 해당 정보를 단독으로 혹은 다른 정보와 결합하여 사용하여 그 정보주체인 개인을 식별할 수 있는 위험이 극히 적다고 판단하는 방법이다. 여기서 말하는 전문가에게 요구되는 특정전문 학위나 자격증 프로그램은 없고, 다만 통계, 수학, 혹은 다른 과학 분야에서 실제적인 경험과 전문지식을 갖추면 된다. 그리고 결정을 할 때도 정량적인 식별 위험에 대한 명시적인 수치 등급은 없다. 따라서 전문가가 허용할 수 있는 매우 작은 위험은 데이터를 활용하는 각자가 개인을 식별하는 능력에 기초해서 정의할 수 있다.

전문가가 익명화된 결과를 다시 판단하는 이유는 이차 활용이 되는 정보의 특성에 따라, 조합에 따라 개인이 재식별되는 경우가 다르기 때문이다. 그리고 해당기관(§b)은 개인식별이 되는 건강정보가 아니라고 결정할 수 있는 경우는 오직 이와 같은 판단을 정당화할 수 있는 방법과 분석결과를 문서화 할 때이다.

FDA의 통제하의 임상적 연구대상의 권리와 안전을 도모하거나, HHS에 의해 지원되는 연구에서도 프라이버시 침해 위험도가 높은 항목으로서의 PHI개념을 참고로 하고 있다.[247]

이상의 내용을 정리하면, PHI가 포함된 자료를 연구에 활용하는 방법은 환자로부터 사용동의를 받는 방법, 연구심의 기관으로부터 사용심의를 면제 받는 방법이며, 환자로부터 사용동의를 받지 않아도 되는 경우는 PHI 정보를 익명화하든지, 제한된 데이터세트(Limited Data Set; 이하 LDS)를 사용하는 방법으로 요약할 수 있다.[248] 직접적 식별자는 삭제되고, 간접 식별자(상세주소, 날짜 등)를 포함

247) HHS Protection of Human Subjects Regulations Title 45 CFR Part 46,; FDA Protection of Human Subjects Regulations Title 21 CFR Parts 50 and 56.

248) HIPAA에는 Limited data set(LDS)를 구성하기 위해서는 직접적 식별자들을 반드시 삭제하여야 한다고 명시되어 있다.; 직접적 식별자(16 항목); 1. 이름 2. 우편번호, 타운, 시, 우편번호를 제외한 주소정보 3. 전화번호 4. 팩스번호 5. 이메일주소 6. 주민등록번호 7. 환자번

하고 있기 때문에 프라이버시 규칙에서 규정하는 익명화된 정보는 아니다. LDS는 공중 보건 및 공익을 목적으로 하는 보건의료 연구를 주 목적으로 하는 경우에 이용한다. 그러므로 LDS를 이차 활용하는 연구자는 LDS 사용계약을 제공기관과 체결한 후, 계약자 상호간 계약범위 내에서 정보를 사용하고 공개할 수 있다. 따라서 이 경우에는 개인 서면동의보다는 데이터 사용계약을 개인정보보호규칙으로 삼고 이를 준수해야 한다. 예를 들면, 연구자는 연구대상자의 개인정보를 식별하려고 하거나 참여자를 접촉해서는 안 된다. 만약 계약외의 정보오용과 공개가 발생할 경우, 제공기관에 보고할 의무가 있다.

HIPAA는 개인정보의 재식별(re-identification)을 허용하는 추가 규정이 있다. 즉 익명화된 건강정보 집합에 고유코드(unique code)를 할당하는 방법이다. 고유코드를 보유할 수 있는 전제조건은 기록 식별코드나 기타 수단이 개인에 관한 정보에서 파생하거나 관련되지 않고, 그 개인으로 식별될 가능성이 없는 경우, 이차 활용기관이 기록 식별코드나 기타 수단을 다른 목적으로 사용하거나 공개하지 않으며, 재식별 기법을 공개하지 않는 경우이다.

5.2.3.3 세이프 하버원칙

미국은 유럽과 무역을 해야 하는 민간분야에서 유럽연합의 개인정보준칙에 따라 개인정보보호 법제를 보충해야하는 상화에 직면하였다. 그래서 2001년 유럽위원회로부터 개인정보보호의 적정성을 확인 받았다고 추정할 수 있는 '세이프 하버(Safe Harbor)' 원칙을 만들었다.[249] 이 원칙을 따를 것인지의 여부는 미국

호 8. 보험증번호 9. 계좌번호 10. 자격/면허증번호 11. 차대번호, 자동차식별번호 12. 의료기기 식별자 및 일련번호 13. URL 14. IP 주소 15. 지문 및 음성을 포함한 생물학적 식별자 16. 얼굴의 전판사진이미지나 그에 상응하는 이미지.

249) European Union (EU) Data Protection Directive of 1995 Frequently Asked Questions, Rebecca Herold, CISM, CISSP, CISA, FLMI, Computer Security Institute, May 2002 issue of

기업들의 선택사항이지만 일단 자발적으로 결정했다면, 그 원칙에 따라 개인정보 취급의 적정성여부를 판단 받게 된다. 관련기업들이 세이프하버 원칙을 자발적으로 준수하겠다고 상무부(Department of Commerce; 이하 DOC)에 신고할 경우 적정성여부를 심사 받는다.

세이프하버 원칙의 골자는 ①고지(Notice): ②선택(Choice): ③제3자 전송(Onward Transfer): ④안전성(Security): ⑤정보의 무결성(Data Integration): ⑥열람(Access): ⑦실행(Enforcement)이다. 특히 민감한 정보가 제3자에게 제공되는 경우 등에는 명백하게 정보주체가 이를 사전 동의해야만 송신할 수 있다.

그러나 여기에도 몇 가지 예외가 적용된다. 즉 정보주체나 타인의 중대한 이익을 위하는 경우, 소송 등의 법적 절차의 경우, 진료의 경우, 비영리단체를 위하는 경우, 고용관계에 사용되는 경우, 이미 공개되어 있는 정보인 경우에는 사전 동의를 제한할 수 있다. 즉 동의가 면제된다.

5.2.3.4 프라이버시 사전영향평가제도

프라이버시에 관한 사전영향 평가의 시초는 1982년 제정된 '컴퓨터 연결과 프라이버시 보호법(Computer Matching and Privacy Protection Act, 1988)'이다.[250] 동 법에서 해당기관의 상급관청들로 구성된 정보완전성위원회(Date Integrity

---

the Alert newsletter,; *The Safe Harbor* was a voluntary self-certification program for U. S. firms. To help bridge the differences between the way the US government approaches privacy issues and the EU Directive, the U.S. Department of Commerce consulted with the European Commission. The Safe Harbor provides a privacy compliance framework and a way for US organizations to avoid experiencing interruptions in their business dealings with the EU, or facing prosecution by the European authorities under European privacy laws.

250) Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (Oct. 18, 1988), codified at 5 U.S.C. §552a note, rev. 1990.; 데이터베이스간의 컴퓨터 매칭을 수행할 때 당해 행정기관이 준수하여야 할 구체적 절차를 규정하고 그 활동을 감독할 자료보호통합위원회를 설립할 것을 요구하고 있다.

Boards)를 만들도록 요구하였다. 그 후 2002년 '전자정부법(E-government Act)'에서는 정부기관이 전자정부 사업을 추진하는 경우에는 사전에 반드시 개인정보 및 프라이버시에 미치는 영향을 분석 및 평가하여 그 대책을 마련할 것을 의무화하였다.[251] 이에 따라 공공기관은 수집되는 개인정보와 수집하는 이유 및 그 용도, 수집된 개인정보를 공유하고자 하는 대상과 정보보호에 관한 사항 등에 대하여 사전영향평가를 실시하고 있다.

미국은 개인정보보호에 관하여 단일한 독립적인 감독기구는 두고 있지 않지만 공공부문에서는 대통령 직속의 관리 예산국(Office of Management and Budget; 이하 OMB)이 예산 편성권을 가지고 강력한 보호체계를 수행하고 있다. 그리고 OMB의 장은 각 정부기관의 프라이버시 사전영향평가를 위한 구체적 정책 및 지침을 개발하여야 하며 범정부적인 프라이버시 사전영향평가의 시행을 감독하여야 한다.[252]

하지만 OMB의 지침에 명시된 '일상적 사용'은 '프라이버시법(Privacy Act 1974)'과 더불어 다른 공공기관과의 정보공유를 허용하는 역외사유를 규정한다. 그러나 OMB의 지침은 권고적일뿐 법적 구속력이 없으며 OMB가 동 법의 준수여부를 감독하는 독립된 기구는 아니다.[253]

OMB가 법적 구속력이 없다는 점은 데이터베이스를 연결하여 정보공유가 될 경우, 충돌하는 이해관계를 조정하거나 형량할 수 없다는 문제로 이어진다. 즉 개인정보를 보호하기 위해서는 행정부가 공동 활용하는 데이터베이스를 통제해야 하는데, OMB는 그러한 역할을 할 수 없다는 것이다. 또 다른 문제점은 공동 활용되는 데이터베이스를 한 기관 내에서 심사하는 것에 대한 규정이 없다는 것이었다. 즉 최소한의 정보만 공개되어야 하고, 정보사용에 대해서는 서면동의가

251) E-government Act 2002. 제208조.

252) E-government Act 2002. 제208조 제(b)항 제(3).

253) David H. Flaherty, 1992, Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States. UNC Press Books.

있어야 하며, 새로운 기록시스템의 설치에 관해서는 의회와 OMB에게 통지되어야만 한다는 법률 규정만 있다. 그리고 이차 활용의 결과로 야기될 수 있는 새로운 유형의 기본권 침해에 관하여는 대안을 줄 수 없다는 비판을 받았다.[254]

5.2.4 생체·의료정보 이차 활용관련 외국 법제도의 비교

유럽연합은 각 회원국 간의 서로 상이한 제도적 차이를 좁히는 방법으로서 독립된 감독기구를 두고 있는데, 그 중에서 민감정보를 포함한 개인정보 보호에 대하여 오래전부터 고민한 나라는 프랑스이다. 프랑스의 경우는 전자정부를 추진할 때 가장 중요한 조건으로 간주한 것이 개인정보보호의 확립이었다. 즉 개인정보를 포함하는 파일을 매칭(Matich files)할 경우가 프라이버시를 침해하는 가장 위협적인 경우라고 보았던 것이다. 그래서 공유를 목적으로 하는 공공정보는 사전에 법률로서 명확하게 정의되어 있어야 하며, 처음에 제출한 목적과 다른 목적을 위해서는 공공정보를 공동 활용할 수 없도록 한 것이다. 프랑스는 개인정보보호기구(CNIL)가 모든 민감정보의 처리 및 축적에 대하여 등록 또는 신고를 통해 흐름을 파악하고 규제하고 있다. 예외를 적용할 때는 CNIL의 의견에 따라야 한다.[255] 한편, 모든 행정문서의 공유를 위하여 별도의 위원회인 CADA와 협력하며, CADA에서 이차 활용에 대한 위법사항을 별도로 모니터링 한다.

유럽연합의 경우, 정보주체의 동의 없는 제3자 제공과 관련하여, 제3자의 정당한 이익을 달성하기 위하여 필요한 범위 내에서 동의를 넓게 인정하고 있다. 다만, '사후거부방식'에 의해 정보주체의 통제권을 인정하고 있다. 이는 포괄적

254) Rubin E. Jr. Cruse, 1991, "Invasions of privacy and computer matching programs: a different perspective", Computer/Law Journal No.11: pp. 461-474.

255) Loi 2000-321 12 Avril 2000 art 5 JORF 13 avril 2000.; ①처리의 목적, ②목적에 따른 보유하는 정보의 특성과 범위, ③개인정보의 보유기간, ④개인정보를 활용하는 사용주체가 등록되어있다.

동의를 허용하는 것으로 최초 공여의 시점에서 받은 동의가 유효할 수 있는 근거는 포괄적 동의가 허용되기 때문이다. 그런데 포괄적 동의가 허용되는 전제조건은 제시되는 향후 연구할 분야와 연구목적에 대해서 윤리심의위원회의 심사를 거치는 것이다.

포괄적 동의에 관하여 유럽연합에서 실시한 2009년의 설문조사 결과를 주목할 필요가 있다. 의생명과학 연구에 참여한 일반인을 대상으로 한 경험조사에서, 사람들은 연구의 공익성이나 투명성에 더 큰 관심을 가졌다.[256] 다시 말하면, 연구의 전문적 내용을 정확하게 이해하고 자발적으로 동의 한 후에는 실제로 그런 연구를 통해 어떤 결과가 도출되며, 자신의 참여가 어떻게 도움이 되었는지에 관심이 더 많았다. 이 점은 바이오뱅크 사업이 공익을 위해 운영된다는 정당성 확보가 매우 중요하며, 인간대상 연구의 참여자들의 이해를 돕는 것이 연구진행에서는 무엇보다 중요하다는 사실이 역설적으로 표현되었다고 할 수 있다.

익명화와 관련해서는 미국의 HIPAA에서 실시하는 전문가 결정방식의 도입이 유효할 수 있다고 본다. 추적조사를 통해 의학적 상관관계를 확인하려는 연구자들은 유전자 정보나 생물학적 검체로부터 분리된 시험대상자의 개인식별정보를 연결할 필요가 있다. 즉 개인식별이 '분리된' 정보나 검체의 재식별을 위하여 '대체 개인식별정보'인 인구통계학적 정보, 생년월일, 우편번호, 진단코드 등을 연결하는 경우를 말한다. 이 경우, 환자로부터의 정보의 수집과 연구자들에게 전달되는 일련의 과정과 정책을 관리·감독하는 사람의 역할이 중요하게 대두된다. 국내에서는 의료기관이 독자적으로 연구를 위하여 어니스트 브로커(honest broker)를 두어 판단하게 하는 경우가 있다.[257]

---

256) Joanna Stjernschantz Forsberg, Mats G. Hansson and Stefan Eriksson, 2009, "Changing Perspectives in Biobank Research: From Individual Rights to Concerns About Public Health Regarding the Return of the Results", European Journal of Human Genetics 17: pp. 1544-1549.

257) Soo-Yong Shin, *et al.*, 2013, "Lessons Learned from Development of De-identification

5.3 비교법적 분석의 결과

제5장에서는 민감정보인 생체·의료정보를 외국에서 어떻게 보호하고, 이차 활용하는지에 관하여 살펴보았다. 생체·의료정보의 이차 활용에 있어 미국과 유럽, 그리고 우리나라의 법률을 비교하여 표 13과 같이 정리하였다.

표 13. '민감정보 사용제한'과 '사전 동의 후 민감정보 제공'에 관한 법률 비교

		2010 미국 HIPAA	2012 유럽연합 데이터보호 규칙	2013 한국 생명윤리 및 안전에 관한법률
일차수집 및 이용		수집제한 원칙 : 전제조건이 명시된 경우에만 수집 목적명시 원칙 : 합법적 목적의 이행 후에는 정보 삭제 이용제한 원칙 : 같은 샘플을 다른 목적을 위해서 사용 할 경우, 나중에 사용할 샘플의 생물학적 정보를 검토한 후 결정		이용제한 원칙
		익명화	익명화/ 가명화	익명화/ 암호화
		사전 동의	사전 동의	사전 동의
		직접수집	단일한 접촉점	직접 수집
이차 활용을 위한 제공	법적 정당성	직접동의 사용심의	이차 활용조건 및 동의 조건 고지	사전 동의
	제3자에게 제공	PHI 익명화 LDS 사용	정보수집 시 고지/ 정보축적과 사용/공개	다른 법에 근거
	민감정보	환자의 권리 1)개시청구권 2)정정청구권 3)실명보고권	수집 및 이용 제한	사전 동의/ 합법적, 명시적 목적에 제한적 사용
	전송을 위한 정보처리	수탁기관의 프라이버시 보호 시스템 보안	익명화 정보보호 디자인	암호화 익명화
	학술연구 목적	LDS 사용계약	개인식별자 삭제된 정보는 동의 면제 프로파일링 금지 합법적 목적에만 사용	개인식별자 삭제된 정보는 동의 면제

System for Biomedical Research in a Korean Tertiary Hospital", Healthcare informatics research 19(2): pp. 102-109.

외국의 입법례에서 각 법률을 나열해서 보여준 이유는 민감정보를 별도 취급하여 특별한 방법으로 보호하고 있다는 것을 보여주고, 그럼에도 불구하고 이차 활용의 필요성에 따라 법제도를 보완하고 있다는 것을 강조하기 위함이다. 우리나라는 1980년의 OECD 개인정보보호원칙을 그대로 가져오며, 유럽연합의 법률체계를 따라 2011년 개인정보보호법에 적용하고 있다. 하지만 법제도도 기술발전 단계를 거치면서 단계적으로 그 개정의 과정이 필요하다고 본다. 특히 이차 활용의 관점에서 최신기술과 함께 드러나는 프라이버시에 대한 우려와 공공정보 이차 활용에 대한 요구에 적절한 대안으로서의 법제도 개선은 절실하다고 본다.

생체·의료정보의 이차 활용을 위한 외국 법제도의 비교결과 다음과 같은 네 가지 측면에서 우리나라 법제도의 문제점을 해결할 수 있는 입법 정책적 함의를 찾을 수 있다.

첫째, 충분한 설명에 근거한 동의와 공익성에 관한 문제이다. '생명윤리 및 안전에 관한 법률'에서의 충분한 설명에 근거한 동의와 '개인정보보호법'에 명시된 개인정보 동의는 별개이다. 개인정보의 정정, 삭제, 폐기는 사전에 서면동의가 면제된 의생명과학연구대상자가 주장 할 수 없는 권리이므로 이들 민감정보 주체들의 협력과 이에 일치하는 법제도가 필요하다. 정보주체들의 협력을 이끌기 위해서는 그것이 동의이든, 동의면제이든 공적인 이익이 사회적 맥락에서 어떻게 개인에게 돌아가는지 공익의 결정과정에 참여할 수 있는 기회가 공정하게 주어져야 한다. 그런 기회를 보장 받도록 하고 개인의 권리를 행사하기 위한 합리적인 판단의 근거를 국가는 보장해야 한다. 이러한 개념은 법적인 절차를 수행할 때 정당성을 얻을 수 있을 것이다. EU 사법재판소에서 강조하듯이, 개인정보보호와 관련한 권리는 절대적 권리는 아니고 사회기능적인 면과 관련되어 고려해야 한다.[258] 공익에 관하여 정보주체와 함께 의사소통하고 법적 정당성을 확보하는 것이 사적

258) EHCR 제8조, TFEU(Treaty on the Functioning of EU) 제16조, EC 헌장 제8조.

권리와 공익의 균형의 원리이다.

둘째, 이차 활용을 위한 익명화에 관한 문제이다. 이차 활용은 다양한 데이터베이스에 보관되어 있는 개인정보를 이용하는 것이다. 우리나라 현행법에서는 개인 식별자를 제거하는 방법, 암호화, 익명화 등을 언급하고 있으나 구체적으로 어떤 식별자를 제거해야 하는지는 명시된 바가 없고 재식별 문제에 대한 조치를 어떻게, 어디까지 해야 하는지도 명시되어 있지 않다. 또한 수집단계에서 부터 익명화된 정보를 수집하는 것과 다른 목적을 위해 제공하는 경우에 개인식별자를 제공하지 않는 것에는 기술적·법적으로 많은 차이가 있다. 게다가 생체·의료정보는 익명으로 수집할 수 없는 경우가 더 많다. 따라서 이를 법적으로 구분할 필요가 있고, 익명화의 유효성에 관하여 기술적 조치를 구체적으로 명시하고 그 절차를 수행하는 체계적인 구조가 마련되어야 한다.

민감정보를 보유·관리하고 이차 활용을 위한 요청에 의한 공유를 하는 공공기관 간에 공동의 규칙이 없는 현실에서, 법적 구속력이 확보된 공동의 규칙 마련은 그동안 소극적이었던 학술연구를 위한 민감정보의 제공에 대한 과도한 프라이버시 침해 우려에 대한 활용과 보호간 균형의 원리이다.[259]

셋째, 서면동의와 감독기구에 관한 문제이다. 정보주체가 공공기관에 맡겨진 정보에 대해서는 자신의 정보이지만 정보의 객체로 머물 수 있다는 측면에서 감독기구의 역할을 재조명할 필요가 있다. 감독기구가 심의하는 서면동의의 면제가 공공정보의 이차 활용에 대한 정당성을 밝히고, 필요하다면 재동의 및 사후 동의를 이끌어내는 제도를 시행할 수 있는 구심점이 되어야 한다. 이는 감독기관 간 상호협력을 통하여 목적에 일치하는 정보를 요청·심의, 제3자에게 전송하는 일련의 절차에 대한 균형의 원리이다.[260]

259) EU General Data Protection Regulation, Brussels, 2012,; TFEU 제16조, 제288조.

넷째, 생체·의료정보 수집에 관한 기술적인 문제이다. 의료기관이나 공공기관 밖에서 개인이 인지하거나 수집동의를 못한 채 수집되는 생체정보나 의료정보는 수집하는 기기를 생산하거나 설계하는 초기 단계에서부터 프라이버시 보호 기능을 내장하는 것이 필요하다. 더욱이 이렇게 수집된 정보가 네트워크나 링크를 통해 연결되거나 전송되는 경우, 정보주체가 알 수 없는 시기에 미래의 목적에 쓰일 수 있으므로 정보주체에게 동의를 강요하거나 정보이용자에게 무조건 프라이버시 보호에 대한 의무 이행을 부담시키는 것은 부당한 측면이 있다. 그러므로 신기술이나 새로운 정보통신시스템을 설계 할 때 미리 가명화 기술을 적용하는 방안을 찾을 필요가 있다. 이렇게 프라이버시 보호에 대한 확신을 주는 적극적인 노력이 공공기관의 운영원칙이 되어야 한다는 것이 공익과 사적 권리의 균형의 원리이다.[261]

비교법적인 분석의 결과로서, 의료가 발전하면 할수록 생체의료정보와 같은 민감정보는 이차 활용되는 측면이 많다는 것을 확인할 수 있었고, 의생명과학 연구에서의 이차활용은 공익성에서 그 정당성을 찾았다. 하지만 정보주체의 권리 보호라는 측면에서는 아무런 제한 없이 활용할 수 있는 것이 아니므로 공익과 사적 권리는 대립된다. 그러므로 법적인 근거와 그 수행절차를 통하여 양쪽의 이익이 구현되도록 하는 것이 중요하다. 또한 법규제와 더불어 정보기술을 다루는 측면에서도 프라이버시 보호 개념이 민감정보의 수집부터 이차 활용까지의 전 과정에 포함되어야 함을 확인하였다.

---

260) EU General Data Protection Regulation, 제7장.

261)Ann Cavoukian, 2009. Privacy by design.; The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.

제6장 생체·의료정보 이차 활용을 위한 개선방안

공공기관이 수집·관리하고 있는 생체·의료정보 이차 활용에서 가장 쟁점이 되는 것은 생체·의료정보의 수집절차상의 문제와 이차 활용을 위한 처리, 동의, 심의의 문제라고 요약할 수 있다. 생체·의료정보를 이차 활용하는데 있어서 공백으로 남아 있는 법적 타당성을 보완하기 위하여 다음과 같은 방안을 제시하고자 한다.

6.1 민감정보의 보호와 이차 활용의 균형점

개인정보호법에 근거하여 개인식별자를 익명화하여 민감정보를 보호하는 방식으로는 개인정보로서 생체·의료정보를 보호하는 정당성을 찾기에는 불충분하였다. 또한 공공정보로서 생체·의료정보를 이차 활용하기위해 정보주체가 수인할 수 있는 근거를 공익성에서 찾기에도 빈약하였다. 나아가 사적 이익과 이차 활용을 통해 얻어지는 공익을 비교 형량하는 절차에서도 정보주체는 그 의사결정 과정에서 배제되어 있었다.

앞서 살펴본 사적 권리와 공익에 비추어 본 생체·의료정보의 보호와 이차 활용의 균형점은 이차 활용을 위한 생체·의료정보의 요청과 제공에 있어서 익명화된 정보를 수집하고, 이차 활용 후에라도 정보주체의 개입이 가능한 사후동의 방식의 도입이 사적 권리를 보장해 주는 법익이 될 수 있다. 정보학적으로는 익명화 및 복원화의 문제를 판단하는 전문가의 개입, 그리고 공공기관 간 공동규제가 가능한 규칙이 필요할 것이다. 이와 더불어 개인정보보호와 공익성을 함께 모색할 수 있는 위원회의 역할의 개선이 필요하다. 그리고 의료기관 밖에서 생체·의료정보를 수집 전송할 수 있는 다양한 기기에 대하여 프라이버시를 고려한 시스템의 설계도 요구된다.

즉 민감정보의 보호와 이차 활용의 균형점 그 균형점을 구현할 수 있는 방안은 공익성, 익명성, 투명성의 확보와 프라이버시 보호 시스템설계로 요약할 수 있다.

6.2 민감정보 처리에 있어서 익명성 확보방안

6.2.1 전문가 결정방식 도입

우리나라 현행법은 개인정보처리자를 규제하고 정보의 수집·처리·제공 단계별로 적용되는 기술적 조치를 규정하고 있다. 즉 개인정보보호법에서 칭하는 개인정보관리자의 업무로 한정되어 있어 이차 활용을 위한 민감정보 처리방법은 언급되어 있지 않다. 다만 우리나라의 인체유래물 은행에서는 익명화 방법에 제거해야 될 개인식별자를 추가 하였지만 그 방법은 여전히 혼란을 주고 있다.

익명화의 한계는 오히려 사전 동의의 필요성을 더욱 강조하게 만든다. 그러나 이차 활용은 사전 동의를 받을 수 없는 경우가 더 많다. 그래서 익명성을 확보하는 기술은 다양한 이해관계자가 함께 결정할 필요가 있다. 또한 의생명과학 연구에서는 개인식별자를 복원하여 개인을 식별하는 것이 필요할 경우도 있다. 복원이 필요한 경우에도 이를 판단하고 연결자를 관리하기 위해서는 익명화된 자료를 검색하고 검토하는 전문가의 개입이 필요하다.

의생명과학연구를 위한 이차 활용을 할 때 필요한 익명화방법에 관해서는 적어도 미국의 HIPAA의 전문가 결정방법을 유의하게 볼 필요가 있다. HIPAA에서 제시한 열여덟 개의 건강정보(Protected Health Information)를 최대한 제거하고 해당분야의 전문가가 그 결과의 신뢰성을 판단하는 방법이다.[262]

---

262) Paul Ohm, 2010, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". UCLA Law Review 57(6): pp. 1701 - 1777: Under the US Health Insurance Portability and Accountability Act (HIPAA), PHI that is linked based on the

이때의 전문가는 개인정보보호법에서 칭하는 개인정보 처리자가 아닌 공공기관에서 의생명과학연구를 위해 제공되는 민감정보를 처리하는 개인정보책임자이다. '책임'을 질 수 있는 직업인을 전문가라고 할 때, 전문직 윤리(professional ethics)는 더욱 강조되며 특별히 정보를 더 가지고 있는 사람의 책임은 더 가중된다.[263] 생체·의료정보를 이차 활용 할 수 있을 만큼의 발전된 기술이라도 그것을 활용하고, 인류에게 도움이 되도록 하는 것은 결국 연구자등 전문가들이다. 이들이 먼저 법의 정신을 이해하고 기술을 판단하도록 함으로써 개인정보의 수탁자이면서 국가의 권력을 위탁받은 책임자가 되어야 해야 할 것이다.

생체 정보와 의료정보를 통합하여 이차 활용하기 위해서는 정보의 발굴 및 정보 공급, 분석도구 개발, 데이터베이스, 시스템구축 등의 일련의 정보산업이 함께 언급되어야만 한다. 따라서 생체·의료정보처리에 관여하는 정보제공자, 소프트웨어 및 분석도구 개발자, 정보처리시스템과 솔루션을 제공하는 정보기술자 등 세 부분의 전문가들의 역할을 적합하게 명시할 필요가 있다.[264]

---

following list of 18 identifiers must be treated with special care: "Encouraging the Use of, and Rethinking Protections for De-Identified (and "Anonymized") Health Data"; Center for Democracy and Technology. June 2009. Retrieved June 12, 2014. "HIPAA: What? De-identification of Protected Health Information (PHI)". HIPAA Research Guide. University of Wisconsin-Madison. August 26, 2003. Retrieved June 12, 2014; De-identified data is coded, with a link to the original, fully identified data set kept by an honest broker. Links exist in coded de-identified data making the data considered indirectly identifiable and not anonymized. Coded de-identified data is not protected by the HIPAA Privacy Rule, but is protected under the Common Rule. The purpose of de-identification and anonymization is to use health care data in larger increments, for research purposes. Universities, government agencies, and private health care entities use such data for research, development and marketing purposes.
http://healthcare.partners.org/phsirb/hipaaglos.htm#g3

263) 정창록, 이일학, 2013. 다산 정약용의 목민심서(牧民心書)에 나타난 자(慈) 개념과 의료윤리, 한국의료윤리학회지 16(3): 281-301면.

264) Sharon Srodin, 2006, Using the Pharmaceutical Literature. Taylor & Francis Group.

6.2.2 공공기관 간 BCR(Binding Corporate Rules) 도입

우리나라 공공기관은 이차 활용을 위하여 각기 다른 특별법을 근거로 하고 있어 공공정보 공동이용에 소극적인 면이 있다. 따라서 공공기관의 개인정보 관리자가 해당 기관의 내부 개인정보 보호 규칙을 잘 준수하면서 동시에 다른 공공기관의 개인정보보호 수준을 신뢰하는 것이 필요하다. 그런 측면에서 BCR 제도는 무엇보다 제3의 수익자(third party beneficiary)의 권리가 보장될 수 있도록 법적 구속력이 있다는 점에서 유용하다. 이와 더불어 하나의 표준화된 규칙을 마련함으로써 시간과 비용을 절약할 수 있는 장점이 있다. 물론 BCR은 법률을 대신하는 것이 아니며 어디까지나 다른 정보보호 장치의 보완적인 용도로서만 이용되어야 한다.

본 연구에서는 유럽공동체 BCR의 사례에서 우선 정보주체에게 정보수집의 목적 및 정보관리자가 누구인지를 고지하는 점을 장점으로 파악하였다. 특히 제3자가 이전을 요청할 때는 정보를 받는 기관이 개인정보보호 감독기관의 승인을 얻어 개인정보를 포함한 정보를 이전할 수 있도록 하고 있다.

아래에서는 유럽공동체의 BCR과 비교할 수 있는 규칙으로서 APEC의 CBPR을 대상으로 하여「BCR 및 CBPR의 개인 데이터 보호 및 프라이버시 자격 요건에 관한 참조문서」[265]를 비교분석하였다. 그 결과, 두 규칙에 대한 공통사항 22가지를 추출하였다. 그 후 공통사항에 대한 설명을 추가 하였다. 공공기관이 BCR 문서를 작성할 때, 다음의 원칙들이 실질적인 절차를 수립하는데 활용되기를 기대한다.

---

265) Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents. 참조.

(1)개인정보관리자의 내부 개인정보 보호 규칙의 목적

• 이전을 위한 개인정보의 처리에 대하여 적절한 보호 수준을 제공하기 위한 것이다.

• 내부 개인정보 보호 규칙으로서 준수해야 하며, 실행 의무로 받아들여져야 한다.

(2)개인정보처리자의 내부 개인정보 보호 규칙의 범위

• 지리적 관할 범위

• 데이터의 성격, (잠재)고객, (잠재)내부직원, 공급자

• 내부 개인정보 보호 규칙의 대상으로서 단위 조직

(3)조직 내부에서의 이행 의무

• 인증을 받으려는 모든 기관은 정보주체와 해당 규제기관이 집행하는 법률에 따라 내부 개인정보 보호 규칙을 만들어 의무사항으로서 준수해야 한다.

(4)법적 의무 이행

• 개인정보처리자의 내부 개인정보 보호 규칙은 공통된 원칙으로써 각 공공기관에 대하여 법 이행의무를 부여하고 있어야한다.

(5)제3자로의 이전에 관한 의무의 이행

• 개인정보의 수령자를 대상으로 해당 내부 개인정보 보호 규칙이 어떻게 집행되는지에 대해 설명할 수 있어야한다.

(6)공공기관의 정보관리자와 위탁 처리자(Processors)와의 관계

• 위탁 처리자를 활용할 경우 정보관리자는 기술적 안전성 및 관리적 조치 등을 충분히 보장할 수 있는 위탁 처리자를 선정하고 준수여부를 보장해야 한다.

• 정보관리자는 위탁처리자에게 안전성, 기밀사항, 규칙을 지도해야한다.

• 정보처리자는 통제자의 지시에 의해서만 개인정보를 처리할 수 있다.

(7)외부 위탁자 및 개인정보처리자로의 이전 및 재 이전의 제한

• 이전하는 개인정보관리자의 내부 개인정보 보호 규칙에도 이전 받는 계약자의 의무요건으로서 '개인정보보호 내용'을 명시해야한다.

(8)용어의 정의

• 작성된 용어는 국내법에 따라 해석되도록 해야 한다.

(9)개인정보의 수집, 처리, 이용

• 개인정보가 정해진 목적에 따라 정당하고 합법적으로 수집 처리되어야 할 것과, 당해 목적과 부합되지 않을 경우에는 처리될 수 없음을 명시해야 한다.

(10)데이터 무결성, 비율적용(proportionality)

• 개인정보의 완전성을 확보해야 하며 최신성을 유지해야한다.

• 모든 관련 당사자에게 수정사항을 교환 할 의무를 포함해야한다.

• 개인정보의 이전 및 심화처리(further processed)시에는 수집목적과 적절성(adequate) 및 관련성(relevant)이 있어야한다.

(11)개인정보 처리에 대한 근거

• 개인정보는 정보주체로부터 충분한 설명에 의한 동의 등 유효한 근거가 있을 때에만 처리될 수 있어야한다.

• 개인정보는 적용되는 법률에 근거하여 일관되게(consistently) 처리돼야 한다.

(12)민감정보의 처리

• 민감정보에 적용될 수 있는 가능한 보호조치를 제시하여야한다.

(13)투명성 및 정보권리의 고지

• 개인 정보의 이전과 처리에 대하여 정보주체가 통지받을 수 있는 방법

• 관리자 및 관리기관 또는 연락처 정보

• 수집된 데이터의 처리 목적

• 데이터 수령자 또는 그 범위

• 정보주체가 갖는 접근권 및 수정권

• 해당 정보에 대한 접근 가능한 방법

• 정보주체로부터 직접 수집되지 아니한 경우, 정보주체에게 고지 할 수 없는 경우 등 예외사항에 대해서 내부 개인정보 보호 규칙이 구체화돼야 한다.

(14)데이터의 접근, 수정, 삭제에 대한 권리, 접근과 수정

• 모든 정보주체는 자신의 개인정보의 보유 여부에 대하여 확인할 수 있

어야 한다.

• 모든 정보주체는 개인정보관리자가 보유한 자신의 모든 개인정보의 사본을 획득할 수 있어야 하며, 이 경우 제약 없이, 합리적인 시간 내에, 과도하지 않은 비용으로 제공돼야 한다.

(15)반대권, 선택권

• 적용되는 법률에 따라 달리 요구되어지는 경우, 개인정보처리자는 해당 적용 법률에 의거하여 정보주체에게 당해 개인정보 처리를 반대하거나 혹은 개인정보가 처리되지 않도록 선택권을 제공해 줄 수 있어야한다.

(16)보안 및 기밀유지

• 사고, 불법 파손, 사고 손실, 변조(alteration), 미승인 된 공개 및 접근, 기타 모든 형태의 불법적 처리에 대한 기술적・관리적 보호조치가 적절히 수행되어야한다.

(17)교육 프로그램

• 해당 개인정보관리자를 대상으로 공통규칙에 관한 적절한 교육 프로그램을 제공해야한다.

(18)모니터링 및 검사 프로그램

• 해당 개인정보관리자의 내부 개인정보 보호 규칙의 적용 및 준수에 대한 모니터링 사항을 명시해야한다.

(19)규정 준수 및 준수여부의 감독

• 해당 개인정보관리자의 내부 개인정보 보호 규칙의 준수여부를 감독 및 확인하기 위하여 적절한 네트워크 및 직위를 제공해야한다.

(20)내부 민원처리

• 그룹의 일부 구성원이 개인정보관리자의 내부 개인정보 보호 규칙을 준수하지 않고 있을 경우 모든 정보주체는 이에 대한 민원요청을 할 수 있다.

(21)개인정보처리자의 내부 개인정보 보호 규칙의 개정

• 개인정보처리자의 내부 개인정보 보호 규칙 또는 담당자 목록에 대한 주요 변경사항 발생 시 모든 그룹 구성원에게 통보해야한다.

(22)유효기간

• 개인정보처리자의 내부 개인정보 보호 규칙에 대한 유효기간을 지정해야 한다.

BCR를 작성할 때에는 정보의 이전 및 처리에 대한 수요를 분석할 수 있는 관리자와, 기술적으로 처리가 가능한지 판단할 수 있는 IT전문가, 규칙을 지킬 의무가 있는 공공기관의 담당자 및 법률전문가가 공동으로 참여하는 것이 바람직하다.[266] 그리고 목적과 정보의 내용에 따라 BCR의 내용을 달리해야 한다. 무엇보다 이를 승인하고 정보 이전 허가서의 기능을 할 수 있는지 여부는 개인정보보호 감독기관이 객관적으로 판단 할 수 있도록 맡기는 것이 바람직할 것이다.

6.2.3 개인정보보호 인증제도 개선

우리나라는 개인정보처리기관에 대한 감독을 미래창조과학부가 맡아서 다른 부처와 기관들에 대한 자료제출 요구 권한을 가지고 정보보호 인증제도를 실시하고 있다. 개인정보보호 인증은 미래창조과학부 소속 인터넷 진흥원에서 시스템 보완과 물리적 보완에 초점을 맞춘 인증항목에 의해 조사한다.

본 연구에서 고찰한 APEC의 CBPR의 사례는 개인정보보호를 위한 내부관리 계획의 수립에서부터 개인정보관리자의 책임성있는 검증을 강조한다.[267] 그래서 각 공공기관에서 내부적인 가이드라인 및 정책을 만들 때, 개인정보처리자의 민원해결 절차, 분쟁해결 절차를 포함하고 있다.

국내의 제도에 이를 적용하려면, 공공기관 간 BCR과 같은 계약은 체결하되,

---

266) White & Case, June 2005, “Binding corporate rules — streamlined and ready for take-off?”, Data Protection and Privacy, White & Case: p.2.

267) APEC : 프로그램 자격요건, Q39: p.24; Q46: p. 26.

실정법으로서의 구속력은 없으므로 업무 효율성을 높이는데 CBPR과 같은 원칙을 보충적으로 사용할 수 있을 것이다. 즉 개인정보인증제도를 개선해 볼 만 하다. 기존에 시행되고 있는 인증 제도가 공공기관으로 그 대상이 확대되는 것이다. 특히 의료기관은 비영리기관으로서 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'에 근거하면 인증대상이 아니므로 실질적으로 민감정보가 수집·관리되는 의료기관에 적용하기 위해서는 개인정보보호 인증 제도를 이용할 수 있다. 예컨대 보건의료분야 부분을 만들고 이차 활용을 위한 정보처리 항목을 추가 할 수 있다.

다만 이 제도는 개인정보보호 감독기구의 승인을 대신해 주는 것은 아니므로, 만약 별도의 승인절차를 위해서는 개인정보보호위원회의 역할이 필요하다. 그러나 대통령직속 개인정보보호위원회는 조사권이 없이 공공부문 개인정보 침해에 대한 시정 조치권만을 가지고 있다. 그리고 민간부문의 분쟁조정 업무는 분쟁조정위원회에서 담당하고 있다. 이러한 감독기구의 분산과 애매한 지위는 공공기관의 개인정보 처리자 및 처리기관에 대한 관리감독에 혼선을 빚게 할 수 있다. 따라서 다음에 기술하는 심의절차의 개선이 필요할 것이다.

6.3 심의절차의 투명성 확보방안

생체·의료정보의 이차 활용에 있어 특이한 점은 개인식별을 필요로 하고, 익명화된 정보를 복원할 필요가 있다는 점이다. 따라서 익명화가 되면, 정보주체의 동의 없이도 이차 활용할 수 있다는 일반 원칙의 조건이 성립되지 않는다. 그러므로 이차 활용의 목적이 사전에 공개되어 공익을 위해 활용한다는 합의와 그 구성원들 사이에 협력을 이끌어내는 절차가 있어야한다.

이러한 절차가 필요한 또 다른 이유는 특정한 연구와 관련하여 중복연구를 피하고 통계적으로 연구의 객관성을 훼손[268]하지 않도록 하려는 목적도 있다.

이러한 노력은 모두 민감정보의 최소처리 및 최소이용을 위해서 필요한 절차가 될 수 있다. 다음에 연구자의 투명성을 확보하기 위한 관리감독의 방식으로 첫째, 개인정보 감독기구의 협력과 둘째, 사후동의 제도 시행을 강조하려고 한다.

6.3.1 개인정보 감독기구 협력

우리나라는 개인정보 보호법 시행에 따라 2011년 9월 30일부터 개인정보보호위원회와 개인정보 분쟁조정위원회가 설립되어 독립적이고 준 사법적인 조정업무를 나누어 담당하고 있다.

우선 개인정보보호위원회는 정책, 제도, 법령개선 같은 개인정보보호정책에 관한 사항을 다루고, 분쟁조정위원회는 개인정보와 관련된 다양한 분쟁이 발생하는 경우에 이를 해결하는 일을 한다. 개인정보보호위원회는 중앙행정기관 등 다른 공공기관에 의한 심의 요청이 있는 경우에 심의·의결하며 공공부문에서의 개인정보 침해에 대해서만 구제기능을 수행한다.

개인정보보호위원회 외에 분쟁조정위원회를 별도로 둘 필요가 있는지는 정책결정사항이라고 할 수 있다. 물론 설립목적이 다르지만 현재 행정자치부 소속으로 분쟁조정위원회가 남아 있는 것은 문제이다. 오히려 개인정보보호위원회 소속의 하부 위원회로 구조를 바꾸어 심의결과를 집행하는 기관의 역할을 하는 것이 더 나아 보인다. 그렇게 하면, 정책과 규제의 분리와 이에 따른 인적구성의 차별화를 극복하고, 분쟁해결의 일관성 및 조절기능을 유지하며, 위상과 역할을 달리함으로서 발생하는 예산낭비를 방지하는 등의 장점도 있다. 또한 두 위원회가 개인정보 보호와 활용을 위해 설립된 기관임을 감안한다면, 이러한 분리 조치는 적절해 보이지 않는다. 오히려 공공정보의 공유로 얻을 수 있는 장점과 야기되는

---

268) Anne Cambon-Thomsen, 2004, “The Social and Cultural Issues of Post-Genomic Human Biobanks”, Nature Reviews Genetics 5: pp. 866-873.

문제에 균형감각을 갖기 위해서는 동일한 기관에서 감독·심의하는 것이 합리적일 것이다.

‘생명윤리 및 안전에 관한법률’ 제7조에 의해 대통령 소속의 국가생명윤리심의위원회가 인간대상 연구의 심의 면제에 관한 사항 및 공용기관생명윤리위원회의 업무에 관한 사항을 심의하고 있다. 공공정보의 이차 활용이 더 많아지고, 인간대상 연구가 더 활발해 지면, 국가생명윤리위원회의 심의 결과와 개인정보보호위원회의 심의 결과가 서로 이견이 있는지 확인할 필요성이 생길 것이다. 특히 이차 활용은 여러 공공기관에서 수집된 정보를 재활용하는 것이므로 기관생명윤리위원회와 관련연구자가 공동으로 이용하는 공용기관생명윤리위원회의 역할이 강조될 수밖에 없다. 따라서 이들 위원회의 의견을 수렴하는 국가생명윤리위원회가 대통령 소속이라는 같은 위상을 가지고 있는 개인정보보호위원회와 협력하여 활용과 보호에 대한 균형을 이끌어 내는 것이 반드시 필요하다고 본다.

6.3.2 사후동의 제도 시행

생체·의료정보는 다양한 목적으로 이차 활용된다. 인간대상 연구, 공중보건 연구, 의료서비스에 대한 연구, 의료전달 체계에 관한 연구, 약물에 관한 연구, 맞춤 의료에 관한 연구 등 다양한 목적에 따라 그 위험의 양상과 정도도 상이하다. 따라서 동의 방법과 면제 형식을 달리할 필요가 있다. 그리고 이러한 변화를 실질적으로 적용한 동의 방식과 승인을 수행하는 절차가 있어야 한다.

수집할 당시에는 목적을 명확히 정의내리기 어려운 의생명과학연구의 경우, 연구대상자들에게 동의를 구하는 목적을 설명하기 힘들다. 따라서 정보주체는 포괄적 동의를 통해 공적 이익을 공감하고, 자기정보에 대한 결정권은 국가에 위임

하는 것에 동의하는 방법을 선택할 수 있다. 포괄적 동의의 방법은 사후 동의이며, 그 내용은 자신이 동의한 내용이 미래 사회의 공익을 위함이라는 것이다. 그리고 실제로 그러한 결과를 가져 올 수 있도록 연구과정 중간에 적절한 시기와 방법으로 연구 내용을 공개하여 지속적인 정당성을 마련해야 한다.

사후 동의로 인해 달라지는 점은 현행법이 충분한 '설명'에 대해서 간과하는 부분이 보충될 수 있다는 것이며 '공익'을 위해서 양보했던 개인의 권리를 정당하게 다시 행사할 수 있다는 점이다. 이때의 사후 동의는 비록 합법적으로 공공기관이 동의 없이 개인정보를 처리 한 후라도 사유가 생기면 언제든지 자신의 정보처리를 중단할 수 있는 거부권이다.

사후 동의가 시행될 때, 가장 필요한 것은 미래의 연구가 내포하고 있는 공적 이익에 대한 신뢰와 그 개인정보를 활용하는 사람들의 책임감이다. 이 책임감은 정보주체가 자신의 권리에 대해서 공익을 위한 정당한 경우라는 일정 범위 내에서 자발적으로 권리제한을 수인하는데 필요한 요청으로서, 우리가 헌혈을 하거나 장기를 기증할 때와 동등하게 이해 될 수 있는 책임감[269]을 말한다.

사후 동의 방식의 수행은 국가생명윤리심의위원회와 개인정보보호위원회가 함께 '민감정보의 이차 활용'에 대한 동의를 수행함이 바람직해 보인다. 왜냐하면 인체유래물과 인체유래물이 수집·보관되어 있는 바이오뱅크의 관리 및 운영체계의 정당성을 수시로 검증해야 하고 여러 공공기관에 수집·보관된 정보를 동시에 고려해야하기 때문이다. 동의와 관련한 감독기관의 역할이 절대적인 중요성을 갖는 또 다른 이유는 공공정보로서의 생체·의료정보를 활용하는 입장과 민감정보로서 생체·의료정보를 보호하는 입장이 조화를 이루어야 하기 때문이다. 이러한 조화가 정부입장에서는 바이오뱅크의 운영에서 함께 공익성을 담보해

269) Ruth Chadwick and Kåre Berg, 2001, "Solidarity and Equity: New Ethical Frameworks for Genetic Databases", Nature Reviews Genetics 2: pp. 318-321.

나가는 방법이 될 수 있고, 정보주체입장에서는 공익에의 참여라는 새로운 흐름으로서 개인정보자기결정권을 행사할 수 있는 토대가 될 수 있을 것이다.

6.4 프라이버시 보호에 적합한 시스템설계방안

다양한 분야, 다양한 기기를 통하여 수집되는 민감정보는 프라이버시 영향평가와 함께 운영된다. 프라이버시 영향평가는 우리나라를 비롯하여 대부분의 개인정보보호 법제를 가지고 있는 나라들이 실시하고 있다. 그러나 법률에 언급된 목적 내에서만 정보가 수집·관리된다고 해서 프라이버시가 저절로 보호되는 것은 아니다. 그래서 이차 활용의 결과로 인해 침해될 수 있는 새로운 유형의 프라이버시에 관해서 공공정보를 공동으로 활용하거나 전송되어 한 곳에 데이터가 모이는 기관에 대해서도 프라이버시 영향 평가를 하는 추세이다.

생체·의료정보는 수집하는 단계부터 기술적인 문제가 파생된다. 의료기관이나 공공기관 밖에서 개인으로부터 수집되는 생체정보나 의료정보가 있기 때문이다. 따라서 생체신호를 수집하는 기기를 생산하거나 설계하는 초기 단계에서부터 프라이버시 보호 기능을 내장하는 것이 필요하다. 즉 신기술이나 새로운 정보통신시스템을 설계 할 때 미리 수집단계에서의 익명화 기술과 활용단계에서의 인증기술이 조우하는 시스템설계이다. 예를 들면, 다양한 데이터 소스로부터 잠재적인 연구를 위해 목표를 가진 데이터베이스를 설계하기 위해서는 데이터의 세부적인 부분까지 개인정보보호와 공정한 사용이 고려된 다양하고 광범위한 사용권한이 필요하다. 본 연구에서는 민감정보의 이차 활용은 무엇보다 정보주체의 인식이 중요하다는 취지에서 캐나다에서 활용하고 있는 개인데이터생태계(personal data ecosystem)의 개념[270]을 적용하고자 한다.

개인데이터생태계란 개인이 정보의 주체이지만 공공서비스를 받기 위해서 공공기관에 자기정보결정권을 맡길 수밖에 없는 비대칭관계를 말한다. 즉 어쩔 수 없이 매일 자신의 개인정보를 수집하고 사용하고 공개하는 공공기관이 자신의 정보사용을 결정하는 비대칭관계를 역전시킬 수 있는 방법을 정보시스템 설계 단계부터 포함시켜서 프라이버시 보호방안을 마련해 보자는 것이다. 예를 들어 사용된 소프트웨어, 데이터 코딩, 데이터 소유권, 일시적인 링크인지 등을 모두 애초부터 고려하는 것이다. 개인데이터 생태계에서 적용할 수 있는 개인정보보호 설계방법으로서 표 14와 같은 것을 고려할 수 있을 것이다.

표 14. 개인데이터생태계에서의 개인정보보호 설계방법 예시

기술적 적용 방법	내용 및 장 점
'민감데이터' 표시 (data marked 'sensitive')	사용자가 선택한 비밀번호로만 열람 가능함.
익명화데이터 접속 (anonymized data tethering)	엑서스할 수 있는 사람을 결정할 수 있음.
네트워크 탭 (network tab)	네트워크 관련자들은 사용자 정보를 개별적으로 열람 가능함. 다른 사용자에게 동일한 정보를 확대 가능함.
조작방지 로그 (temper-resistant audit logs)	데이터베이스 관리자조차도 변형할 수 없을 만큼 조작방지 로그 방식
한 방향 암호화 (one-way encryption)	다른 시스템과의 연동에서 부정오류 방지 매번 로그인 할 때 마다 비밀 번호를 바꾸어야함.
삭제 버튼 ('delete' button)	플랫폼에 delete botton을 심어 놓아 시스템로그에서는 사용자 데이터를 남기지 않음.
정보주체 계약 (personal's Legal Framework)	이차 활용을 위한 전송 시 법률에 의한 정보주체의 동의, 정보변경, 삭제 등을 한다는 법률 효력이 있는 계약서를 첨부함.

270) Ann Cavoukian, 2013, Information & Privacy Commissioner Ontario, Canada. http://www.privacybydesign.ca/index.php/paper/personal-data-ecosystem-pde-privacy-design-approach-individuals-pursuit-radical-control/

개인데이터생태계에서 의생명과학 연구를 위하여 우선 적용할 수 있는 방법 중에는 개별적으로 일회성으로 필요한 데이터와 공동 사용하는 데이터 세트에 대한 동의 절차가 각각 별도로 포함된 시스템 설계가 있을 수 있다. 그리고 개인 스스로가 자신의 정보의 중심이 되도록 기술적 방안을 확보하는 방안의 예는 지문, 홍채 등을 이용한 개인인증과 같은 바이오 매트릭스 인증기술을 도입하는 것이다. 이때 개인의 특징을 추출한 템플릿 데이터의 저장부터 파기에 이르기까지의 운용 가이드라인을 정하는 것이다.

기술적 방안의 장점은 공적 기금으로 조성된 의료시스템의 계획과 관리과정뿐만 아니라 민간부문이나 비영리 의료기관에서 수집된 정보가 이차 활용의 목적으로 공공기관으로 유입될 때에도 중개기관에 의해 똑같은 절차로 수집될 수 있다는 것이다. 하지만 이 경우에도 네트워크나 링크를 통해 연결되거나 전송되는 민감정보에 대한 별도의 규칙을 적용해야 한다. 예를 들면, 디지털 영상에서 얻어진 개인정보를 추상적인 기호로 전환한다거나 얼굴을 대상물체로 식별하여 추출한 데이터를 암호화하여 저장하는 것이다. 그렇게 하면 원래 영상과 인물을 제외시킨 영상에서 암호화된 영상을 추출하여 식별을 원할 때만 정보관리자가 식별하는 대상의 내용을 복호화 할 수 있을 것이다.

6.5 사회적 합의에 기초한 법제개선 방안

생체·의료정보의 활용과 보호는 여러 법률에서 그 근거를 찾을 수 있으나 특정한 정보주체의 권리행사와 프라이버시 침해와는 무관하다. 즉 사전 동의 혹은 동의 면제로 이분화 되어 있는 현재의 동의 절차만으로는 이차 활용대상 정보의 주체들은 자기결정권을 충분히 행사하지 못하는 측면이 있다.

우리나라는 아직까지 국민 개개인이 자신의 정보사용에 대한 권리와 자유에 대하여 공론화하고 이차 활용에 대한 인식을 조사한 바가 없다. 그래서 정보주체가 쉽게 개인정보자기결정권을 행사하는 것도 아니면서 동시에 이차 활용을 통한 공익 목적의 연구도 제한되어 결국 양쪽 모두에게 별다른 이익도 얻을 수 없는 것이 현실이다. 그러므로 문제 해결의 실마리를 찾기 위해서는 무엇보다 정보주체의 의사를 탐구하는 노력이 선행되어야 할 것이다. 예를 들어 인간대상연구의 모든 연구자가 연구대상자로부터 동의를 획득해야 한다면, 동의서 획득에 대한 방법론이 담겨 있어야 한다.

정보주체와 의생명과학연구를 하는 연구자들이 협의 할 수 있는 장(場)이 마련되어야 하는데, 이때의 협의는 양쪽이 이성적 담론을 통해 규범적 맥락을 이해하고 합의에 이를 수 있는 절차를 포함한다. 합의과정을 정보보호기구가 돕고, 이 과정에서 도출된 쟁점이 법적 기초를 만들 때 반영되어야 할 것이다. 이렇게 의사소통적 합리성에 따라 만들어진 법은 정당성을 갖추게 될 것이다.

공익과 사적 이익에 대한 비판적 검토와 반성적 수용을 하기 위하여 하버마스의 입장을 따라 상호주관적인 의사소통의 합리성을 이론적 근거로 가져왔다. 하버마스의 합리성 이론은 현실분석을 통해 도출된 결과와 문제점에 관해 보편타당한 관점에서 평가 할 수 있는 규범적 척도를 가지고 있다. 하버마스가 말하는 정당성을 획득하기 위한 담론 원리와 같은 것이다. 실천적 담론의 참여자로서 모든 관련자들의 동의를 얻을 수 있도록 절차적 과정이 마련되어야 한다는 연구자의 주장이 설득력을 갖는다고 보았다. 왜냐하면 하버마스의 설명처럼 생활 세계와 체계가 끊어지지 않고 지속될 수 있는 연결고리 기능을 법이 담당하며 법의 정당성은 의사소통적 합리성에 있기 때문이다.[271] 이 합리성에는 상호적인 비판도 있지만 반성적 수용도 있다.

271) 선우현, 앞의 논문(각주 38): 88-111면.

일련의 절차를 그대로 따라가다 보면, 보호와 활용의 양측 모두가 수용할 수 있는 보편타당한 규범임을 증명되고, 스스로 실천력의 원천으로 작용되는 것이 과정이 되어야한다. 이러한 과정을 거쳐야 이차 활용과 보호를 위한 합의의 결과는 정보주체 누구나가 인지할 수 있으며, 동시에 실천하기에 너무 어렵지 않은 내용이 될 것이며, 동시에 사적 권리와 공익의 균형을 이루는 것임을 증명할 수도 있을 것이다.

공공기관간의 합목적적인 결론은 비록 지극히 민감한 정보일지라도 정보주체 스스로와 타인 그리고 공동체 모두의 이익을 위해 활용한다는 것을 증명해야 공익성이라는 조건을 충족할 수 있으며, 이를 함께 현실세계로 구현할 수 있는 법제도의 방향 전환에도 근거가 될 수 있다. 이러한 공익성은 비록 이차 활용의 혜택이 정보주체에게 금방 되돌아가지 않더라도 동의 면제를 수용할 수 있는 공공정보의 이차활용을 위한 법제도의 정당성으로 작용될 수 있을 것이다. 그래서 민감정보일지라도 이차 활용을 하기 위해서는 이차 활용 대상 정보, 동의면제 정보, 동의 절차 등의 결정과 관련하여 공적 담론을 거쳐 입법화할 수 있는 가능성을 기대할 수 있다.

제7장 결론

본 논문에서는 개인정보자기결정권이 자신에 관한 정보의 흐름을 자율적으로 결정할 수 있는 사적 권리임을 논증하였다. 그리고 생체·의료정보와 같이 특별히 개인정보자기결정권이 더욱 강조되는 민감한 정보의 이차 활용에 대하여 왜 그러한 사적 권리가 보호되어야 하는지, 어떻게 보호될 수 있는지 고찰하였다.

개인이 갖는 자신의 정보에 대한 자기결정권은 절대적이고도 무제한적인 지배를 의미하는 것이 아니다. 공공기관이 수집·관리하고 있는 개인정보는 동의가 면제된 채 활용되기도 한다. 공익의 목적이라는 조건이 이차 활용을 수인하는 정당성의 근거이다.

공공정보는 공공기관 간에는 정보주체의 동의 없이 활용할 수 있으나, 건강보험심사평가원, 중앙암 등록 본부, 질병관리본부, 국민건강보험공단, 한국보건사회연구원, 국립보건원등에 수집·관리되고 있는 생체·의료정보는 민감정보라는 특수성을 지니고 있다. 이들 정보는 대부분 의생명과학연구를 위해 이차 활용되는데 예를 들면, 질병의 진단과 치료, 의료보험 심사, 의료시스템의 개편의 근거자료, 바이오의약연구, 코호트 연구, 의료서비스의 미충족 연구, 공중보건 등이다.

생체·의료정보가 프라이버시에 특별히 취약한 이유는 정보자체가 개인식별성이 있을 뿐만 아니라 이차 활용을 통하여 익명성이 재식별 되기도 하기 때문이다. 이차 활용을 통하여 얻을 수 있는 많은 이점과 공익성에도 불구하고, 정보주체의 권리를 보호해야하는 이유도 바로 여기에 있다. 그래서 생체·의료정보의 이차 활용에 대한 요구와 가용성이 증가 할수록 이차 활용으로 인해 유발될 수 있는 프라이버시 침해에 대한 우려도 커지게 되면서 보호와 활용이라는 두 측면은 더욱 첨예하게 대립된다.

우리나라는 민감정보의 활용에 대해서는 분야별 특별법을 적용하고, 보호에 관해서는 일반법으로서 민간과 공공부문의 모든 개인정보를 보호하는 법률체계를 가지고 있다. 하지만 이차 활용의 결과로 야기 될 수 있는 새로운 유형의 프라이버시 침해에 관해서는 현재의 법제도적 보호 방안의 한계가 있다는 문제의식을 가지고 다음 네 가지 관점에서 이를 검토하였다.

첫째, 어떠한 경우에도 충분한 설명에 근거한 동의가 정보주체의 개인정보 자기결정권을 보장해주는가? 둘째, 이차 활용에서도 개인정보 비식별 조치가 익명성을 보장해 줄 수 있는가? 셋째, 개인정보 보호를 위한 일반법과 공공정보 활용을 위한 특별법이 공존하는 법률체계에서 서면 동의와 면제에 관한 법 적용이 서로 모순되지 않는가? 넷째, 이차 활용에 있어 법제도와 운영절차 이외에 프라이버시 보호방법은 없는가?

위와 같은 질문에 답하는 기준으로서 우선 기본권 제한의 일반원칙인 '비례의 원칙'이 준수되는지를 검토하였다. 생체·의료정보를 이차 활용하는 의생명과학 연구는 특정한 정보에 대한 사적 이익을 미래의 결과를 위하여 동의를 면제하는 방법으로 제한해야 되는 경우이다. 이렇게 국민의 기본권을 제한할 때는 보호하려는 공익과 침해되는 사적 권리를 비교 형량하여 보호되는 공익이 커야 한다는 헌법상의 원칙을 지켜야 한다. 하지만 그 인과관계를 입증하기 힘든 측면이 있다. 왜냐하면 개인정보자기결정권과 연구결과를 통한 공익의 실현은 부분적으로는 서로 상충되는 가치도 있지만 동시에 중첩되기도 하며 결과적으로 공익안에서 추구되는 개인의 사적 권리도 있기 때문이다.

본 연구에서는 민감정보 주체의 사적 권리를 보호하면서 이차 활용도 가능한 원리로서 균형의 원리를 파악하였다. 이차 활용의 법적 타당성을 공익성과 익명성, 그리고 투명성으로 보았다. 공익을 위해서 동의 면제를 수인하고, 이차 활용을 통하여 재식별될 수 있는 위험성을 익명성을 보전할 수 있는 기술적 규제적

방법을 보완적용하며, 동의 면제를 심의·의결하는 절차를 투명하게 하는 것이다.

민감정보 보호와 이차 활용의 균형점을 고찰하기 위하여 국제기구와 외국 법률체계를 비교분석하였다. 그 규율방식이나 사회적 여건, 기술 수준의 차이에도 불구하고 정보사회의 문제를 대처하는 각국의 법제는 상당히 근접해가는 경향임을 확인할 수 있었다.

생체·의료정보는 정보주체의 동의 없이는 원칙적으로 목적 외로 활용하지 못한다. 그러나 '충분한 설명에 근거한 동의'는 동의하는 시점에서는 특정 분야의 미래 연구결과에 대한 충분한 설명이나 이해가 이루어지기 힘들며, 따라서 이를 충분한 설명에 근거한 동의라고 말할 수는 없는 측면이 있다. 또한 유전자정보를 포함하는 생체정보의 경우, 이차 활용 후에 가계연관성으로 인하여 연구대상자가 아닌 경우에도 연구에 참여한 것과 같은 결과가 될 수 있다. 이 경우에는 정보주체의 동의가 없는 채 이차 활용이 되는 샘이다.

또한 생체·의료정보를 이차 활용한 결과는 공익을 위해서 쓰인다. 그렇다면, 사적 권리 보호와 공익을 위한 이차 활용이라는 이익은 상반된 입장으로서 양자택일을 할 문제가 아니다. 개인정보자기결정권으로서 보호하려했던 사적 권리는 공익을 위해 양보되며, 이차 활용으로서 도달하려고 했던 공익은 민감한 정보주체에게 가장 먼저 혜택이 돌아갈 수 있기 때문이다. 양쪽 모두가 목표로 하는 것이 공동체의 이익이면서 동시에 개개인의 프라이버시의 보호이기도하다. 그래서 민감정보의 보호와 이차 활용은 법익의 균형이 요청된다.

공익이라는 목적 때문에 훼손 될 수 있는 사적 권리를 행사하도록 할 수 있도록 하는 법제도의 개선과 이차활용으로 보전하기 어려운 익명성을 보전하는 규칙, 민감정보의 수집에서부터 전송에까지 적용할 수 있는 시스템의 디자인에 대한 개선방안을 제시하였다.

구체적으로 공공정보 중 생체·의료정보의 이차 활용을 위하여 공익성에 근거한 자기결정권의 제한방식으로서 사후 동의, 민감정보 처리는 익명성을 보장하기위한 전문가 결정방법의 도입, 공공기관의 정보제공은 투명성을 보장하기위한 개인정보보호 감독기구의 협력 방안이다. 그리고 우선 필요한 각 공공기관 간 구속력 있는 절차의 확보 방안의 도입을 제안하였다. 또한 생체정보를 수집하는 시스템 설계 시 미리 네트워킹을 하는 기술에 프라이버시 보호라는 개념을 적용한 솔루션을 포함할 것을 제안하였다.

공공정보 중에서 생체·의료정보는 공익의 목적을 위해 활용되는 경우가 많고, 대량의 정보가 활용된다는 특징이 있다. 최근에는 정부가 주도하는 의생명과학 연구가 점점 더 늘어나고 있다. 국가적 수준에서 추진되는 바이오뱅크 사업은 정책시행에 의해 성패가 좌우 될 수 있다. 그래서 바이오뱅크와 관련된 연구는 장기간에 걸쳐 일관된 국민적 신뢰를 얻은 일이 무엇보다 중요하다. 하지만 동시에 정보주체인 국민의 참여가 없이는 완성되기 힘들다. 그런 의미에서 정보주체의 참여 방안을 모색한 것은 본 연구의 성과라고 할 수 있을 것이다.

본 연구의 한계점으로는 생체·의료정보가 실제로 활용되는 목적과 사례별로 이차 활용 때문에 침해가 예상되는 부분을 구체적으로 정리해 내지 못한 것이다.

향후에는 이차 활용의 목적 별로 활용 대상 민감정보 세트 구성을 시도하고, 수집부터 결과 분석, 연구 결과의 공유까지 관여하는 위원회의 역할과 이를 입법화하는 연구가 필요할 것이다.

참 고 문 헌

[국내문헌]

1. 단행본

(1) 국내서

곽윤직. 2005. 민법총칙(민법강의) 제7판. 서울 : 박영사.

권영성. 2002. 헌법학원론. 서울 : 법문사.

김정오 외. 2012. 법철학-이론과 쟁점. 서울 : 박영사.

김철수. 2000. 헌법학개론. 서울 : 박영사.

박정자. 2008. 시선은 권력이다. 서울 : 기파랑.

박정훈. 2005. 행정법의 체계와 방법론. 서울 : 박영사.

백윤철·김상겸. 2006. 미국의 의료정보보호에 대한 연구. 고양 : 한국학술정보.

성낙인. 1998. 언론정보법. 서울 : 나남출판사.

성낙인. 2008. 헌법학. 파주 : 법문사.

양창수. 2000. 민법입문(신수판). 서울 : 박영사.

최대권. 1999. 헌법학강의. 서울 : 박영사.

최송화. 2002. 공익론: 공법적 연구. 서울 : 서울대학교 출판부.

홍정선. 2012. 행정법원론(상). 서울 : 박영사.

허영. 2005. 헌법이론과 헌법. 서울 : 박영사.

(2) 번역서

로렌스 레식. 2002. 코드: 사이버공간의 법이론. 김정오 역. 서울 : 나남출판.

로렌스 레식. 2006. 코드 2.0. 김정오 역. 서울 : 나남출판.

로베르토 웅거. 1994. 근대사회에서의 법. 김정오 역. 서울 : 삼영사.

마이클 샌델. 2010. 왜 도덕인가. 안진환·이수경 역. 서울 : 한국경제신문.

마이클 샌델. 2010. 정의란 무엇인가. 이창신 역. 서울 : 김영사.

2. 논문

강경근. 2005. “情報保護의 憲法規範的 接近과 展望”, 공법학연구 제6권 제2호.

권건보. 2004. “自己情報統制權에 관한 硏究: 公共部門에서의 個人情報保護를 중심으로”, 서울대학교 대학원. 박사학위 논문.

권헌영. 2004. “전자정부환경에서의 개인정보보호법제에 관한 연구”, 연세대학교 대학원. 박사학위논문.

권형준. 2003. "정보통신의 발달과 헌법상의 과제", 한일법학 제22권.

김도균. 2006. “법 원리로서의 공익 -자유공화주의 공익관의 시각에서-”, 서울대학교 법학. 제47권 제3호.

김도균. 2007. “법적 이익형량의 구조와 정당화문제”, 서울대학교 법학. 제48권 제2호.

김도균. 2012. “한국 법질서와 정의론: 공정과 공평, 그리고 운의 평등-시론(試論)”, 서울대학교 법학. 제53권 제1호.

김용섭. 2001. “정보공개와 개인정보보호의 충돌과 조화”, 공법연구 제29권 제3호.

김유환. 2006. “영미에서의 공익개념과 공익의 법문제화-행정법의 변화와 대응”, 서울대학교법학연구소. 서울대학교 법학 제47권 제3호.

김일환. 2001. “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 공법연구 제29권 제3호.

김종철. 2001. “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 인터넷법률 4호.

김형준. 1999. “온라인 법률정보시스템의 구축에 따른 법적 문제- 정보공개와 사생활보호를 중심으로-”, 중앙대학교 법학연구소. 법학논문집 제23집 제2호.

박균성. 2006. “프랑스 행정법상 공익개념”, 서울대학교 법학. 제47권 제3호.

박병섭. 2002. “독일의 개인정보보호 제도에 관한 연구”, 민주법학 25호.

박원환・황조연. 2004. “통계자료의 비밀보호를 위한 익명화 방법들”, 통계연구. 제9권 제2호

변재옥. 1991. “현대사회에 있어서 정보공개와 인권보장”, 저스티스 제24권 제2호.

서계원. 2005. “정보프라이버시와 개인정보의 보호”, 세계헌법연구 제11권 제1호.

선우현. 1998. "합리성이론으로서 하버마스의 비판적 사회이론", 서울대학교 대학원. 박사학위논문.

양화식. 2008. "생활세계, 체계 그리고 법- ‘하버마스의 의사소통행위이론’을 중심으로", 법철학연구 제11권 제2호.

윤광석. 2012. "행정정보공동이용제도의 개선방안에 관한 연구", 정보화정책 제19권 제4호.

이계만 외. 2011. “한국의 공익개념 연구: 공익관련 법률내용 분석을 중심으로”, 한국정책과학학회보 제15권 제2호.

이광윤 외. 2009. "공공부문의 개인정보 활용・공개 및 보호에 관한 법제 연구 - 프랑스, 독일, 영국, 일본을 중심으로-", 정보보호 법제연구 시리즈 1. 한국정보보호진흥원.

이상욱·조은희. 2011. “바이오뱅크의 바람직한 운영을 위한 공론화의 필요성”, 생명윤리 제12권 제1호.

이인영. 2006. “유네스코 ‘생명윤리와 인권보편선언’의 권고사항과 국내 실천을 위한 제언”, 과학기술법연구 제12권 제1호.

이인호. 2001. “온라인 프라이버시 침해기술과 보호기술의 법적 함축”, 법학논문집 25집 2호.

이인호. 2005. “미국의 개인정보보호법제에 대한 분석과 시사점”, 중앙대학교. 법학논문집 제29권 제1호.

이한주. 2013. “개인정보보호위원회 제도의 문제점과 개선방안 -프랑스 CNIL과의 비교를 통하여-”, 경북대학교, 법학논고 제41집.

임진희 외. 2012. “의무기록관리의 현황과 개선방안”, 정보관리학회지 제29권 제3호.

정규원. 2010. “건강정보의 이차적 이용”, 한양대학교 법학연구소. 법학논총 제27권 제1호.

정재황. 2006. “프랑스 법에서의 개인정보의 보호에 관한 연구”, 공법연구 제34집 제4호 제1권.

정창록・이일학. 2013. “다산 정약용의『목민심서(牧民心書)』에 나타난 자(慈) 개념과 의료윤리”, 한국의료윤리학회지 제16권 제3호.

최송화. 1996. “행정법상 공익개념의 전개와 의의”, 현대헌법학이론우제 이명구 박사 회갑 기념논문집 II.

최송화. 1999. “공익개념의 법문제화: 행정법적 문제로서의 공익”, 서울대학교 법학 제40권 제2호.

폴크마르 괴츠. 1997. “세계화와 21세기를 위한 법 : 제3주제 발표논문 ; 유럽법의 일반원칙으로서 비례원칙과 신뢰보호원칙”, 서울대학교 법학 제 38권 3·4호.

한상법. 1979. “프라이버시의 권리”, 동국대학교 논문집 제34집.

황인호. 2002. “개인정보보호제도에서의 규제에 관한 연구”, 공법연구 제30권 제4호.

3. 보고서

개인정보보호법제 개선을 위한 정책연구보고서. 2013. 서울: 프라이버시 정책연구포럼.

국가기술지도(NTRM) 비전II 건강한 생명사회 지향 제2권. 2002. 서울: 과학기술부.

생명공학육성시행계획 Bio-vision 2016. 2014. 서울: 미래창조과학부 외.

전자정부법의 이해와 해설. 2001. 서울: 안전행정부.

국내 보건의료 이차자료원 활용. 2013. 서울: 한국보건의료연구원.

정부 3.0과 공공데이터 개방전략. 2013. 서울: 한국지역정보개발원.

아이폰의 사회경제적 파급효과 분석. 2012. 서울: KT 경제경영연구소.

[외국문헌]

1. 단행본

Arendt, Hannah. 2013. The human condition. University of Chicago Press: Chicago, USA.

Barry, Brain M. 1965. Political Argument: A Reissue with New Introduction. University of California Press: California, USA.

Bennett, Colin J. 1992. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Cornell University Press: Ithaca, NY, USA.

Bennett, Colin J. and Raab, Charles D. 2006. The Governance of Privacy-Policy Instrument in Global Perspective. MIT Press: Cambridge MA, USA.

Bohman, James. 1997. Deliberative democracy: Essays on reason and politics. MIT press: Cambridge MA, USA.

Brody, Baruch A. 1988. The Ethics of Biomedical Research: An International Perspective. Oxford University Press: Oxford, UK.

Calhoun, Craig. edited by Walter W. Powell and Elisabeth S. Clemens. 1998. The Public Good as a Social and Cultural Project. Yale University Press: New Haven, USA.

Cavoukian, Ann. 2009. Privacy by design *Take the Challenge*. Information and Privacy Commissioner of Ontario: Toronto, Canada.

Cavoukian, Ann. 2013. Information & Privacy. Commissioner Ontario: Toronto, Canada.

Cavoukian, Ann, et al., 2011. Privacy by ReDesign. Building a Better Legacy: Toronto, Canada.

Chapman, John W. and Shapiro, Ian (eds). 1993. Democratic Community: Nomos XXXV, New York University: New York, USA.

Cooley, Thomas McIntyre, 1878, A Treatise on the Law of Torts or the Wrongs Which Arise Independently of Contract, 1st edition. Callaghan and Company: Chicago, USA.

Corrigan, Oonagh and Tutton, Richard. 2004. Genetic databases: Socio-ethical issues in the collection and use of DNA. Routledge: Kentucky, USA.

Danielson, Peter. 1996. Pseudonyms, mailbots, and virtual letterheads: The evolution of computer-mediated ethics. Philosophical perspectives on computer-mediated communication. State University of New York Press: Albany, USA.

Emmanuel, Ezekiel J., et al., 2003. Ethical and Regulatory Aspects of Clinical Research: Readings and Comments. Johns Hopkins University Press: Baltimore, USA.

Flaherty, David H. 1992. Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States. UNC Press: North Carolina, USA.

Flathman, Richard E. 1966. The public interest: An essay concerning the normative discourse of politics. Wiley: New Jersey, USA.

Gutmann, Amy and Thompson, Dennis F. 1996. Democracy and disagreement. Harvard University Press: Cambridge MA, USA.

Habermas, Jürgen. 1983. Discourse Ethics: Notes on a Program of Philosophical Justification. Christian Lenhardt & Shierry Weber Nicholsen translation. 1990. Moral Consciousness and Communicative Action. MIT Press: Cambridge MA, USA.

Held, Virginia. 1970. The Public Interest and Individual Interests. Basic Books: New York, USA.

Jürgen Habermas, Translated by Frederick Lawrence. 1987. Der Philosophische Diskurs der Moderne: Zwölf Vorlesungen. MIT Press: Cambridge MA, USA.

Hirschman, Albert O. 1992. Rival Views of Market Society and Other Recent Essays. Harvard University Press: Cambridge MA, USA.

Kuppinger, Martin. 2012. Life Management Platforms: Control and Privacy for Personal Data. KuppingerCole: Wiesbaden, Germany.

Kymlicka, Will. 2002. Debates in Contemporary Political Philosophy. Oxford University Press: Oxford, UK.

Marx, Gary T. 1989. Undercover: Police surveillance in America. University of California Press: Oakland, CA, USA.

McLean, Lain and McMillan, Alistair. 2009. The concise Oxford dictionary of politics. Oxford University Press: Oxford, UK.

Noveck, Beth Simone. 2009. Wiki Government: How Technology Can Make Government Better, Democracy Stronger, and Citizens more Powerful. R.

Donnelley Harrisonburg: Virginia, USA.

OECD. 2006. Digital broadband content: public sector information. OECD Digital Economy Papers No. 112. OECD Publishing: Paris, France.

Pettit, Philip. 2004. Justice and Democracy. Cambridge University Press: Cambridge, UK.

Piateski, Gregory and Frawley, William. 1991. Knowledge discovery in databases. MIT press: Cambridge MA, USA.

Powell, Walter W. and Clemens, Elisabeth S. (eds). 1998. Private Action and the Public Good. Yale University Press: New Haven CT, USA.

Rachels, James. 2003. The Elements of Moral Philosophy Fourth Edition. McGraw-Hill Companies: New York, USA.

Rawls, John. 1999. A Theory of Justice Revised Edition. Belknap Press: Cambridge MA, USA.

Reid, Elizabeth M. 1991. Electropolis: Communication and community on internet relay chat. University of Melbourne: Melbourne, Australia.

Sadurski, Wojciech. 1985. Giving desert its due: Social justice and legal theory Vol. 2. Springer: New York City, USA.

Sandel, Michael J. 1982. Liberalism and the Limits of Justice. Cambridge University Press: Cambridge, UK.

Solove, Daniel. 2008. Understanding privacy. Harvard University Press: Cambridge MA, USA.

Srodin, Sharon. 2006. Using the Pharmaceutical Literature. Taylor & Francis Group: New York, USA.

Trousseau Fenoll et Haas, G. 2000. Internet et protection des donnés personnelles. Litec: Paris, France.

Van Dijk, Pieter, Hoof, Godefridus J. H. and Van Hoof, G. J. H. 1998. Theory and practice of the European Convention on Human Rights. Kluwer Law International: Alphen aan den Rijn, Netherlands.

Waldo, Dwight. 2006. The administrative state: A study of the political theory of American public administration. Transaction Publishers: New Jersey, USA.

Warren, Samuel D. & Brandeis, Louis D. 1890. The Right to Privacy. Harvard Law Review Vol. 4. Cambridge Press: Massachusetts, USA.

Westin, Alan F. 1970. Privacy and freedom. Atheneum: New York, USA.

Zika, Eleni. et al. 2010. Biobanks in Europe: prospects for harmonisation and networking. Institute for Prospective and Technological Studies. European Commission: Brussels, Belgium.

2. 논문

1000 Genomes Project Consortium. 2010. "A map of human genome variation from population-scale sequencing". Nature 467.

Anderlik, Mary R. and Rothstein, Mark A. 2001. "Privacy and confidentiality of

genetic information: what rules for the new science?". Annual Review of Genomics and Human Genetics No. 2.

Annas, George J. 2003. "HIPAA Regulations – A New Era of Medical-Record Privacy?". The new england journal of medicine 348;15.

Barnes, Colin. 1991. “Disabled people in Britain: A case for anti-discrimination legislation for disabled people”. London: Hurst/BCODP.

Tutton, Richard. 2010. "Biobanking: Social, Political and Ethical Aspects". Encyclopedia of Life Sciences. John Wiley & Sons: Chichester, UK.

Belanger, France and Hiller, Janine S. 2006. "A framework for e-government: privacy implications". Business process management journal No. 12.

Bignami, Francesca. 2007. "European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining". BCL Rev. No. 48.

Cambon-Thomsen, Anne. 2004. "The Social and Cultural Issues of Post-Genomic Human Biobanks". Nature Reviews Genetics 5.

Caulfield, Timothy, et al. 2008. "Research ethics recommendations for whole-genome research: consensus statement". PLoS biology No. 6.

Caulfield, Timothy. 2006. "Should donors be allowed to give broad consent to future biobank research?". The Lancet Oncology Volume 7 Issue 3.

Chadwick, Ruth and Berg, Kåre. 2001. "Ideality and Equity: New Ethical Frameworks for Genetic Databases". Nature Reviews Genetics 2.

Chlapowski, Francis S. 1991. "The Constitutional Protection of Informational

Privacy". Boston University Law Review 133.

Cottone, Rocco R. 2001. "A social constructivism model of ethical decision making in counseling". Journal of Counseling & Development No. 79(1).

Cruse, Rubin E. Jr. 1991. "Invasions of privacy and computer matching programs: a different perspective". Computer/Law Journal 11.

Duncan, George T., et al. 2001. "Disclosure Risk vs. Data Utility: : The R-U confidentiality map in Multivariate Settings". National Institute of Statistical Sciences. Carnegie Mellon University.

Elger, Bernice S. and Caplan, Arthur L. 2006. "Consent and anonymization in research involving biobanks: differing terms and norms present serious barriers to an international framework". EMBO reports No. 7(7).

ENCODE Project Consortium, 2007. "Identification and analysis of functional elements in 1% of the human genome by the ENCODE pilot project". Nature 447.

Forsberg, Joanna Stjernschantz, Hansson, Mats G. and Eriksson, Stefan. 2009. "Changing Perspectives in Biobank Research: From Individual Rights to Concerns About Public Health Regarding the Return of the Results". European Journal of Human Genetics 17.

Frazer, Kelly A., et al. 2009. "Human genetic variation and its contribution to complex traits", Nature Reviews Genetics No. 10.

Greely, Hank T. 1999. "Breaking the stalemate: a prospective regulatory framework for unforeseen research uses of human tissue samples and health information". Wake Forest Law Rev. Volume 34 No. 3.

Gross, Hyman. 1967. "The Concept of Privacy". 42 N.Y.U.L. Rev. 34.

Habermas, Jürgen. 1995. "Reconciliation Through the Public use of Reason: Remarks on John Rawls's Political Liberalism". The Journal of Philosophy Volume 92 No. 3.

Hoeyer, Klaus L. 2003. "Science is really needed-that's all I know: Informed Consent and the Non-verbal Practices of Collecting Blood for Genetic Research in Northern Sweden". New Genetics and Society Volume 22 No. 3.

Kang, Jerry. 1998. "Information Privacy in Cyberspace Transactions". Stanford Law Review No. 50.

Kuner, Christopher. 2005. "Using Binding Corporate Rules for International Data Transfers: The ICC Report". Electronic Banking Law and Commerce Report. Glasser Legal Works Volume 9 No. 8.

Miller, Leslie J. 1980. "Informed consent". JAMA Volume 244 No. 18.

Norberg, Patricia A. and Horne, Daniel R.(eds). 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors". Journal of Consumer Affairs Volume 41 Issue 1.

Ohm, Paul. 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization". UCLA Law Review 57.

Pollicino, Oreste. 2008. "European Arrest Warrant and Constitutional Principles of the Member States: a Case Law-Based Outline in the Attempt to Strike the Right Balance between Interacting Legal Systems". German Law Journal Volume 09 No. 10.

Rose, Hilary. 2006. "From Hype to Mothballs in Four Years: Troubles in the Development of Large-Scale DNA Biobanks in Europe". Community Genetics 9.

Rosenbaum, Joseph I. 1998. "Privacy on the Internet: Whose Information Is It Anyway?". Jurimetrics Vol. 38 No. 4.

Rosenbloom, Kate R., et al. 2009. "ENCODE whole-genome data in the UCSC Genome Browser". Nucleic Acids Research Volume 38.

Ruth Chadwick and Sarah Wilson, 2004. "Genomic Databases as Global Public Goods?". Res Publication Volume 10 No. 2.

Shapiro, Ian. 1989. "Constructing Politics". Political Theory Volume 17 No. 3.

Shin, Soo-Yong, et al. 2013. "Lessons Learned from Development of De-identification System for Biomedical Research in a Korean Tertiary Hospital". Healthcare informatics research Volume 19 No. 2.

Toth, Akos G. 1992. "The principle of subsidiarity in the Maastricht Treaty". Common Market Law Review No. 29.

Walther, Joseph B. and Burgoon, Judee K. 1992. "Relational communication in computer mediated interaction". Human communication research Volume 19 No. 1.

Wheeler, David A.(eds). 2008. "The complete genome of an individual by massively parallel DNA sequencing". Nature 452.

3. 보고서

Avis sur les propositions de réforme da la protection des données Charter of Fundamental Rights of the European Union 2012

European Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data 2012

European Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification 2009

EU-US Workshop on Safe Harbor Framework Bridging Differences in Approaches to Data Protection 2005

OECD A Workshop on Access to Public Sector Information and Content 2006

OECD A workshop on public sector information held to prepare the OECD Recommendation 2008

UN E-Government Surveys 2010, 2012

UNESCO International Bioethics Committee, Public Hearings Day on Human Genetic Data. FINAL REPORT. 2003

UNESCO National Bioethics Advisory Commission, Ethical and policy issues in research involving human participants. Report and Recommendations Volume I. 2001

[법률관련 인터넷 웹 사이트]

Constitutional Court of Korea

Cornell University Law School

elaw.klri.re.kr

EUR-Lex

European Public Sector Information Platform

French Administration Directory

International Covenant on Civil and Political Rights

International Covenant on Economic, Social and Cultural Rights

Korea Legislation Research Institute

Online database of Westlaw

Statutes of the Republic Korea

The Official Journal of the European Union

Universal Declaration of Human Rights

[판례]

대법원 1994. 03. 08. 선고 92누 1728

대법원 1998. 01. 23. 선고 97도 2124

대법원 1998. 07. 24. 선고 96다 42789

서울고등법원 1995. 08. 24. 선고 94구39262

헌법재판소 1990. 09. 03. 선고 89헌가95

헌법재판소 1991. 05. 13. 선고 89헌가97

헌법재판소 1998. 02. 27. 선고 95헌바59

헌법재판소 1998. 12. 24. 선고 89헌마214, 90헌바16, 97헌바78

헌법재판소 2002. 10. 31. 선고 99헌바40, 2002헌바50

헌법재판소 2002. 12. 28. 선고 2002헌마52

헌법재판소 2005. 05. 26. 선고 99헌마513

헌법재판소 2005. 07. 21. 선고 2003헌마282

헌법재판소 2005. 11. 24. 선고 2005헌마112

헌법재판소 2005. 12. 22. 선고 2005헌마19

헌법재판소 2007. 05. 31. 선고 2005헌마1139

헌법재판소 2008. 10. 30. 선고 2006헌마1401등

헌법재판소 2009. 09. 24. 선고 2007헌마1092

헌법재판소 2009. 10. 29. 선고 2008헌마257

헌법재판소 2010. 05. 27. 선고 2008헌마663

헌법재판소 2010. 09. 30. 선고 2008헌바132

헌법재판소 2011. 12. 29. 선고 2010헌마293

헌법재판소 2012. 08. 23. 선고 2010헌마47

헌법재판소 판례집 17-2

헌법재판소 판례집 785

헌법재판소 판례집 799-800

Carter vs. Broadlawns Medical Center, 667 F. Supp. 1269. 1987

Dudgeon vs. United Kingdom, case 52. 1981

Griswold vs. Connecticut, 381 U.S. 479. 1965

[법률]

한국

개인정보 보호법 2011

공공기관의 운영에 관한 법률 2007

공공기관의 정보공개에 관한 법률 2004

공공데이터의 제공 및 이용 활성화에 관한 법률 2013

국가배상법 2009

국민건강 증진법 1995

생명윤리 및 안전에 관한 법률 2012

신용정보의 이용 및 보호에 관한 법률 2009

전자정부법 2010

정보통신망 이용촉진 및 정보보호 등에 관한 법률 2010

행정규제기본법 2010

헌법 1987

U.S.A

American Recovery and Reinvestment Act 2009

Cable Communications Policy Act 1984

Child Online Privacy Protection Act 1998

Communications Assistance for Law Enforcement Act 1994

Computer Matching and Privacy Protection Act 1988

Computer Security Act 1987

Driver's Privacy Protection Act 1994

E-government Act 2002

Electronic Communications Privacy Act 1986

Employee Polygraph Protection Act 1988

Fair Credit Reporting Act 1970

Family Education Fights and Privacy Act 1974

Federal Information Security Management Act 2002

Freedom of Information Act 1974

Gramm-Leach-Bliley Act 1996

Guidance Regarding Methods for De-identification of Protected Health Insurance Portability and Accountability Act 1996

Patriot Act 2001

Privacy Act 1974

Privacy Protection Act 1980

Right to Financial Privacy Act 1978

Telecommunications Act 1996

Telephone Consumer Protection Act 1991

Video Privacy Protection Act 1988

FRANCE

Décret n° 2007-1220 du 10 août 2007

LOI n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 2009

LOI n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures 2009

LOI n° 2000-321 12 Avril 2000 art 5 JORF 13 avril 2000

LOI n° 78-753 du 17 Juillet 1978, Loi portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal 1978

LOI n° 78-17 du 6 Janvier 1978, relative à L'informatique, aux fichiers et aux libertés 1978

LOI n° 78-17 du 6 Janvier 1978, relative à L'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004

THE COUNCIL OF EUROPE

European Commission Decision 2001/497/EC

European Commission Decision 2002/16/EC

European Commission Decision 2004/915/EC

European Commission Regulation No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws 2004

European Commission Regulation No 444/2009 of the European Parliament and of the Council 2009

European Convention for the Protection of Human Rights and Fundamental Freedoms 1950

Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981

European Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine 1997

European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Transborder Data Flows 2001

European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 2008

THE EUROPEAN UNION

Directive 95/46/EC the protection of individuals with regards to the processing of personal data and the free movement of such data 1995

Directive 2002/22/EC universal service and users' rights relating to electronic communications networks and services 2002

Directive 2002/58/EC the processing of personal data and the protection of privacy in the electronic communications sector 2002

Directive 2006/24/EC Data Retention Directive 2006

Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services 2009

EU General Data Protection Regulation 2012

European Union Amending Council Regulation No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States 2009

European Union Charter of Fundamental Rights of the European Union Official Journal of the European Communities 2000

Treaty of Lisbon 2007

Treaty on the Functioning of the European Union 2012

APEC

APEC Cross-border Privacy Enforcement Arrangement 2004

APEC Privacy Framework 2004

OECD

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980

ABSTRACT

A Study of Legal System for Secondary Use of Public Information

- Focusing on Secondary Use of Bio or Medical Information -

Park, Mi Jeong
Interdisciplinary Program in
Medical Law and Ethics
The Graduate School
Yonsei University

The aim of this dissertation is to suggest how to strike a balance between the benefits of secondary use of personal information and rights of self-determination for other purposes that within frameworks of personal data protection laws, policy and technologies.

This study critically examine the appropriateness of limiting the right of self-determination in the context of secondary use of public information by a third party for purposes other than data collection. Particularly, the research sought to find common ground between private rights and public interest by specifying privacy issues which could be threatened by secondary use of

sensitive information such as bio or medical information.

Each public agency uses aggregated databases which enable extraction of new meanings and utilization of individual dataset. While not new, these issues play increasingly critical and complex roles given that the Information and Communication Technology Revolution has created a dilemma regarding individual privacy. The nature of the utilization of public data from the database by various public agencies causes them to hold and collect personal information beyond the primary purposes in common databases as secondary use of personal information, incurring serious cases of legal violation of information usage.

The idea concerning privacy and public interest is embedded within a complementary 'using vs. protecting' concept that is not trusted by the owner(s) of the data. There is clearly a need to consider whether the Government is balancing this critically important relationship between data subjects and personal information and whether the current approach is fit for its purpose. As the secondary use of personal information is randomly scattered in the database of the public and collected beyond primary purposes, the minimized use of personal information protected by common law is likely to be violated with the absent clarity in the norms of secondary usage of personal information. Laws to protect personal information protect the interests of the people by requiring consent at every step of information process. Secondary use, however, does not require consent according to a special law that exempts such condition. The problem is exacerbated when every public agency adheres to different

special laws that reflect the objectives of each agency.

On the basis that secondary use of public information has its objective in public interest, literature review was conducted to understand relevant theories for reaching equilibrium between private rights and public interest.

Especially, the special nature of secondary use of bio and medical information collected and owned by public agencies; then, issues raised by the current law in force were analyzed in comparison with precedents in international organizations and foreign laws.

The careful reviewed foreign laws for protecting personal information in public sectors were analyzed via comparison method from the following perspectives: agreement based on full explanation, personal information control right, anonymity for secondary use, broad consent, embodied in privacy by system design, and personal information protection commission.

The review and analysis conducted in this study led to the following conclusions. Review of prior studies on public interest identified that when the operative law does not clearly identify the underlying principles of public interest, it is necessary to critically investigate via public determination process whether both public and individual rights were equally protected.

Essentially all bio or medical information in public agencies are sensitive and require protection in varying degrees. Theoretically, only limited processing of such information is allowed, and no special laws can exempt consent. In other words, priority is given to a subject's right of self-determination. In practice, however, the majority of bio or medical

information for secondary use in biomedical research had been provided by public agencies upon request. The current special law in place exempts written consent upon approval of Institutional Bioethics Committee, thereby allowing researchers to utilize data for secondary use without consenting process. Nonetheless, in such case of exemption, the principle of proportionality should be met by allowing a subject to practice his or her right of self-determination.

Accordingly, achieving a common objective through secondary use of information must begin by sharing common legal restriction across agencies. For this purpose, this study proposed to adopt a single regulation method that has legally binding cooperate rules.

Another condition for secondary use of bio or medical information in absence of consent is de-identification. De-identified information may be regarded as a solution for protecting privacy through anonymization. Several methods could be taken to promote anonymity. Information with identifying data stripped is no longer sensitive. However, a single, concrete anonymization method is required as bio or medical information itself includes identifying data. In so doing criteria anonymization evaluation can be added to certificate personal information management system. In effort to ensure anonymity, expert-determined method must be added for re-identification.

Restricting the right of self-determination on sensitive information such as bio or medical information must notify subjects the purposes in which their information will serve and how the information is being processed. Whether

purpose is justifiable for the sake of public is directly related to the roles of Data Protection Authorities which deliberates the process of secondary use.

In the new phase of the secondary use of public information, this study attempts to balance between public interest and private rights as well as 'using' and 'protecting' through the following suggestions: the review procedures to ensure the data subject's rights including the broad consent to entrust personal data processing in case of substitution; common rules to stipulate the anonymity; the consensus decision making processes to ensure the public interest; and privacy-preserving embedded systems to collecting and sharing sensitive information.

Key words: public information, secondary use, right to privacy, personal information, anonymization, personal information privacy policy, sensitive information, data protection authority, biobank.